2010

Defense Acquisition Guidebook
Dated: August 5, 2010

This PDF version of the Defense Acquisition Guidebook (DAG) is current as of August 5, 2010. A new/updated PDF of theDAG will be posted on or about the 5th of each month or as needed. The online DAG is a living document that will be updated whenever necessary. Consequently, the PDF version may not contain the most current guidance. We suggestyou use the online version whenever possible. https://dag.dau.mil

Acquisition professionals should use this Guidebook as a reference source supporting their management responsibilities

guidebook@dau.mil
Defense Acquisition University
8/11/2010

DEFENSE ACQUISITION GUIDEBOOK

Foreword

The Defense Acquisition System exists to manage the Nation's investments in technologies, programs, and product support necessary to achieve the National Security Strategy and support the United States Armed Forces. In that context, our continued objective is to rapidly acquire quality products that satisfy user needs with measurable improvements to mission capability at a fair and reasonable price. The fundamental principles and procedures that the Department follows in achieving those objectives are described in DoD Directive 5000.01 and DoD Instruction 5000.02.

The Defense Acquisition Guidebook is designed to complement those policy documents by providing the acquisition workforce with discretionary best practice that should be tailored to the needs of each program.

Acquisition professionals should use this Guidebook as a reference source supporting their management responsibilities. As an "on-line" resource, the information is limited only by the user's interest or need. Some chapters contain general content; they provide individual topic discussions and describe processes and considerations that will improve the effectiveness of program planning. Some chapters may provide a tutorial on the application of these topics to the acquisition framework. Depending on the subject matter, a chapter may contain general background information, tutorial discussions, and/or discussions of the detailed requirements for each milestone decision and phase. All chapters contain non-mandatory staff expectations for satisfying the mandatory requirements in DoD Instruction 5000.02

Each chapter is designed to improve understanding of the acquisition process and ensure adequate knowledge of the statutory and regulatory requirements associated with the process. Discussions, explanations, and electronic links to related information enable the "reader" to be efficient, effective, innovative, and disciplined, and to responsively provide warfighting capability. Each chapter lists potential ways the program manager or assigned manager can satisfy mandatory process requirements and meet staff expectations for other activities. Differences of view regarding discretionary practice will be resolved by the Milestone Decision Authority.

The Guidebook is intended to be an electronic reference source rather than a "book." The "reader" "navigates" the information instead of "leafing" through hundreds of physical, collated pages. "Navigation" is electronic movement through the reference system.

Chapter 1, Department of Defense Decision Support Systems, presents an overview of the Defense Department's decision support systems for strategic planning and resource allocation, the determination of capability needs, and the acquisition of systems.

Chapter 2, Defense Acquisition Program Goals and Strategy, discusses acquisition program goals and the topics the program manager should consider in developing a strategy for the acquisition program. It addresses the required information associated with the Acquisition Program Baseline, the Technology Development Strategy, and the program's Acquisition Strategy.

Chapter 3, Affordability and Life-cycle Resource Estimates, addresses acquisition program affordability and resource estimation.

Chapter 4, Systems Engineering, covers the system design issues facing a program manager, and details the systems engineering processes that aid the program manager in designing an integrated system that results in a balanced capability solution.

Chapter 5, Life-cycle Logistics, provides the program manager with a description of Life-cycle Logistics and its application throughout the system life-cycle, from concept to disposal.

Chapter 6, Human Systems Integration, addresses the human systems elements of the systems engineering process. It will help the program manager design and develop systems that effectively and affordably integrate with human capabilities and limitations; and it makes the program manager aware of the staff resources available to assist in this endeavor.

Chapter 7, Acquiring Information Technology, Including National Security Systems, explains how the Department of Defense complies with statutory and regulatory requirements for acquiring Information Technology and National Security Systems and in using a network-centric strategy to transform DoD warfighting, business, and intelligence capabilities. The chapter also provides descriptions and explanations of the Clinger-Cohen Act, the Business Management Modernization Program and many other associated topics and concepts, and discusses many of the activities that enable the development of net-centric systems.

Chapter 8, Intelligence, Counterintelligence, and Security Support, describes program manager responsibilities regarding research and technology protection to prevent inadvertent technology transfer, and provides guidance for and describes the support available for protecting those technologies.

Chapter 9, Integrated Test and Evaluation, discusses many of the topics associated with test and evaluation, to include oversight, Developmental Test and Evaluation, Operational Test and Evaluation, and Live Fire Test and Evaluation. The chapter enables the program manager to develop a robust, integrated test and evaluation strategy to assess operational effectiveness and suitability, and to support program decisions.

Chapter 10, Decisions, Assessments, and Periodic Reporting, prepares the program manager and Milestone Decision Authority to execute their respective management and oversight responsibilities.

Chapter 11, Program Management Activities, explains the additional activities and decisions required of the program manager, not otherwise discussed in earlier chapters of this Guidebook.

DEFENSE ACQUISITION GUIDEBOOK
Chapter 1 -- Department of Defense Decision Support Systems

1.0. Overview

1.0.1. Purpose

This chapter provides background information about the environment in which the Department of Defense must operate to acquire new or modified materiel or services.

1.0.2. Contents

Section 1.1 presents an overview of each of the three, principal, decision support systems used in the Department of Defense to acquire materiel and services, and describes the integration of those systems. Sections 1.2 through 1.4 provide details of each of these systems: Section 1.2 discusses the Planning, Programming, Budgeting, and Execution process, employed by the Department of Defense to conduct strategic planning and make resource allocation decisions; Section 1.3 discusses the Joint Capabilities Integration and Development System used to determine military capability needs; and Section 1.4 discusses the formal Defense Acquisition System used to acquire that capability.

1.1. Integration of the DoD Decision Support Systems

The Department of Defense has three principal decision-making support systems, all of which have been significantly revised over the past few years. These systems are the following:

Planning, Programming, Budgeting and Execution (PPBE) Process - The Department's strategic planning, program development, and resource determination process. The PPBE process is used to craft plans and programs that satisfy the demands of the National Security Strategy within resource constraints.

Joint Capabilities Integration and Development System (JCIDS) - The systematic method established by the Chairman of the Joint Chiefs of Staff for identifying, assessing, and prioritizing gaps in joint warfighting capabilities and recommending potential solution approaches to resolve these gaps. CJCS Instruction 3170.01 and the JCIDS Manual describe the policies and procedures for the requirements process.

Defense Acquisition System - The management process by which the Department acquires weapon systems and automated information systems. Although the system is based on centralized policies and principles, it allows for decentralized and streamlined execution of acquisition activities. This approach provides flexibility and encourages innovation, while maintaining strict emphasis on discipline and accountability.

Illustrated together in Figure 1.1.F1, the three systems provide an integrated approach to strategic planning, identification of needs for military capabilities, systems acquisition, and program and budget development. The next three sections provide brief introductions to each of these decision support systems.

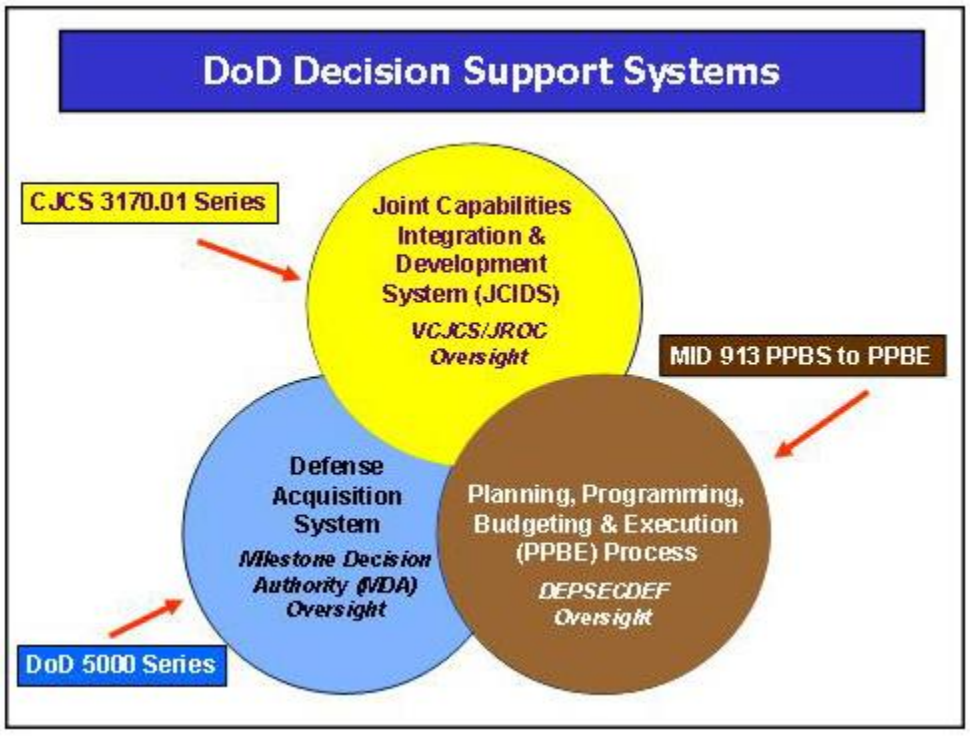


Figure 1.1.F1. DoD Decision Support Systems

1.2. Planning, Programming, Budgeting and Execution (PPBE) Process

The purpose of the PPBE process is to allocate resources within the Department of Defense. It is important for program managers and their staffs to be aware of the nature and timing of each of the events in the PPBE process, since they may be called upon to provide critical information that could be important to program funding and success.

In the PPBE process, the Secretary of Defense establishes policies, strategy, and prioritized goals for the Department, which are subsequently used to guide resource allocation decisions that balance the guidance with fiscal constraints. The PPBE process consists of four distinct but overlapping phases:

Planning. The planning phase of PPBE is a collaborative effort by the Office of the Secretary of Defense and the Joint Staff, in coordination with DoD components. It begins with a resource-informed articulation of national defense policies and military strategy known as the Guidance for the Development of the Force (GDF). The GDF is used to lead the overall planning process. This process results in fiscally constrained guidance and priorities - for military forces, modernization, readiness and sustainability, and supports business processes and infrastructure activities - for program development in a document known as the Joint Programming Guidance. The Joint Programming Guidance is the link between planning and programming, and it provides guidance to the DoD Components (military departments and defense agencies) for the development of their program proposals, known as the Program Objective Memorandum (POM).

Programming. The programming phase begins with the development of a POM by each DoD Component. This development seeks to construct a balanced set of programs that respond to the guidance and priorities of the Joint Programming Guidance within fiscal constraints. When completed, the POM provides a fairly detailed and comprehensive description of the proposed programs, including a time-phased allocation of resources (forces, funding, and manpower) by program projected six years into the future. In addition, the DoD Component may describe important programs not fully funded (or not funded at all) in the POM, and assess the risks associated with the shortfalls. The senior leadership in OSD and the Joint Staff review each POM to help integrate the DoD Component POMs into an overall coherent defense program. In addition, the OSD staff and the Joint Staff can raise issues with selected portions of any POM, or any funding shortfalls in the POM, and propose alternatives with marginal adjustments to resources. Issues not resolved at lower levels are forwarded to the Secretary for decision, and the resulting decisions are documented in the Program Decision Memorandum.

Budgeting. The budgeting phase of PPBE occurs concurrently with the programming phase; each DoD Component submits its proposed budget estimate simultaneously with its POM. The budget converts the programmatic view into the format of the congressional appropriation structure, along with associated budget justification documents. The budget projects resources only two years into the future, but with considerably more financial details than the POM. Upon submission, each budget estimate is reviewed by analysts from the office of the Under Secretary of Defense (Comptroller) and the Office of Management and Budget (OMB). Their review

ensures that programs are funded in accordance with current financial policies, and are properly and reasonably priced. The review also ensures that the budget documentation is adequate to justify the programs presented to the Congress. Typically, the analysts provide the DoD Components with written questions in advance of formal hearings where the analysts review and discuss the budget details. After the hearings, each analyst prepares a decision document (known as a Program Budget Decision, or PBD) for the programs and/or appropriations under his or her area of responsibility. The PBD proposes financial adjustments to address any issues or problems identified during the associated budget hearing. The PBDs are staffed for comment and forwarded to the Deputy Secretary of Defense for decisions. These decisions are then reflected in an updated budget submission provided to the OMB. After that, the overall DoD budget is provided as part of the President's Budget request to the Congress.

Execution. The execution review occurs simultaneously with the program and budget reviews. The execution review provides feedback to the senior leadership concerning the effectiveness of current and prior resource allocations. Over time, metrics are being developed to support the execution review that will measure actual output versus planned performance for defense programs. To the extent performance goals of an existing program are not being met, the execution review may lead to recommendations to adjust resources and/or restructure programs to achieve desired performance goals. PPBE Biennial Cycles. In 2003, the Department adjusted its planning, programming and budgeting procedures to support a two-year cycle that results in two-year budgets. The revised process is described in Management Initiative Decision (MID) 913, dated May 22, 2003. The concept in MID 913 is consistent with submission of a biennial DoD budget that is part of the President's Budget request to Congress for even-numbered fiscal years (FY) (e.g., the FY 2008 President's Budget, submitted to Congress in February 2007, contained justification material for both FY 2008 and FY 2009). In this cycle, the even-numbered years are called on-years, while the odd-numbered years are called off-years. Figure 1.2.F1 displays a nominal timeline for the PPBE phases in an on-year.

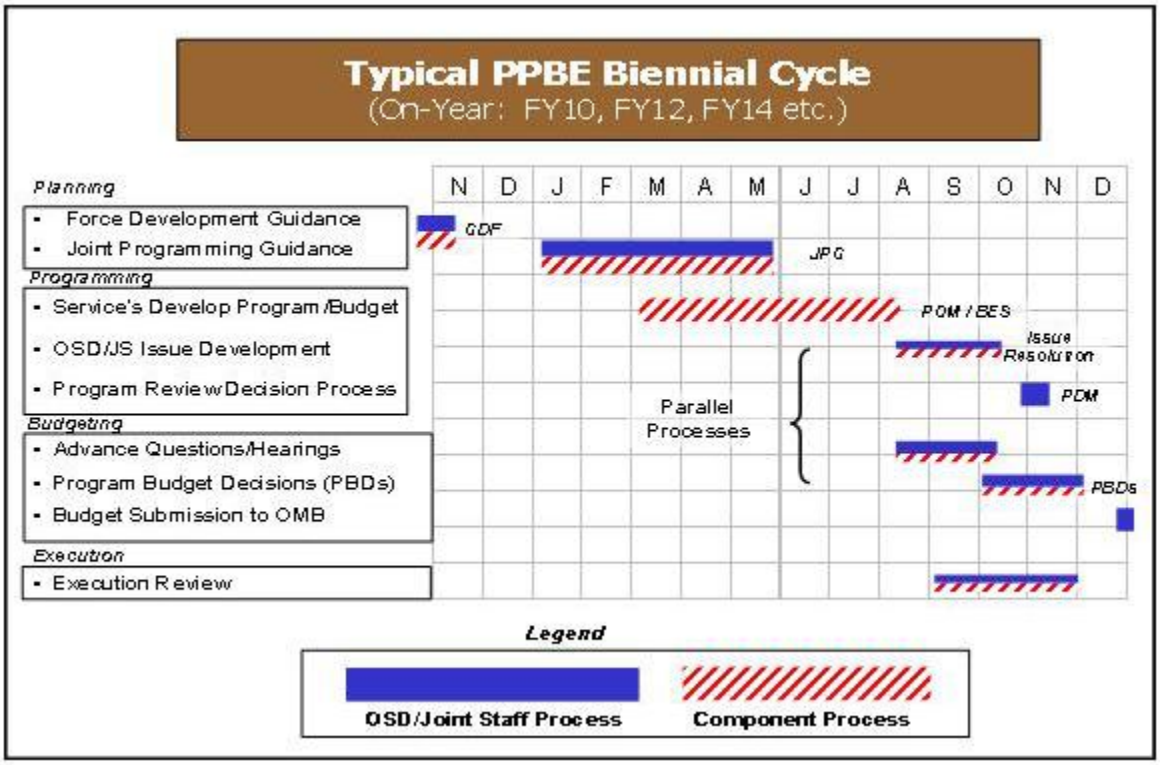


Figure 1.2.F1. Typical PPBE Biennial Cycle, "On-Year"

In practice, Congress does not actually provide the Department with biennial appropriations. An amended budget justification must be submitted for the second year of the original biennial request so that Congress will appropriate funds for that second year. The Department uses a restricted process in the off-year to develop an amended budget that allows for only modest program or budget adjustments. Figure 1.2.F2 displays a nominal timeline for the limited off-year process.

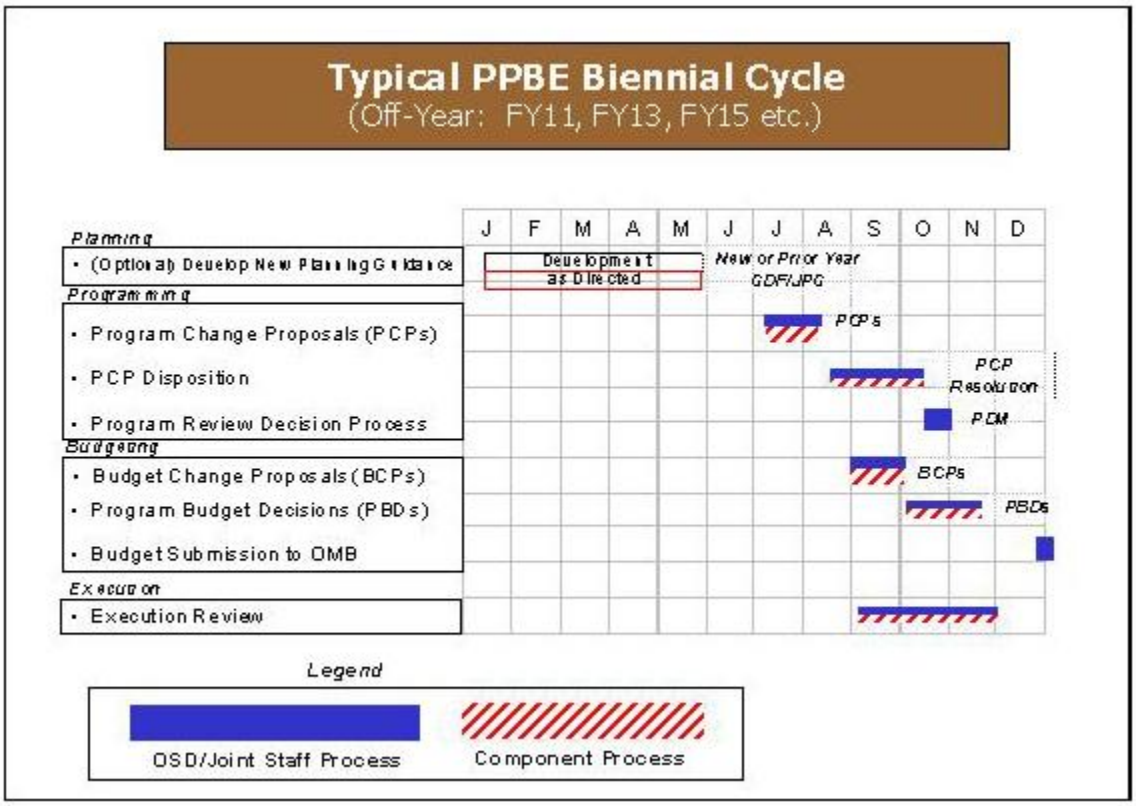


Figure 1.2.F2. Typical PPBE Biennial Cycle, "Off-Year"

Minimum changes to policy, strategy, or fiscal guidance are intended for the off-year. There may be no issuance of revised Guidance for the Development of the Force or Joint Programming Guidance. If revised Joint Programming Guidance is provided, it would contain only minor revisions (although it could direct studies to support major decisions on strategy or program choices for the future GDF/JPG). In the off-year, the DoD Components do not provide revised POMs or budget estimates. Instead, the DoD Components are allowed to submit Program Change Proposals (PCP) and/or Budget Change Proposals (BCP) to account for fact-of-life changes (e.g., program cost increases or schedule delays). BCPs and PCPs are limited to a single issue and must identify resource reductions to offset any program or budget cost growth. PCPs address issues over a multi-year period, whereas BCPs address issues focused on the upcoming budget year. PCPs are reviewed in a manner similar to on-year program issues, and BCPs are resolved through the issuance and staffing of PBDs.

From a larger perspective, the biennial PPBE cycle is designed to support and implement policy and strategy initiatives for each new four-year presidential administration. Figure 1.2.F3 depicts alignment of the biennial PPBE cycle over a four-year term.

Figure 1.2.F3. PPBE Two-Year Cycles Corresponding to Four-Year Presidential Terms

In the first year of the administration, the President establishes a revised National Security Strategy, which establishes: (1) the worldwide interests, goals, and objectives that are vital to the national security; and (2) the foreign policy, worldwide commitments, and national defense capabilities necessary to implement the national security goals and objectives. Once the new administration's National Security Strategy is established, the Secretary of Defense, in consultation with the Chairman of the Joint Chiefs of Staff, leads the Quadrennial Defense Review (QDR). The QDR is a comprehensive review of all elements of defense policy and strategy needed to support the national security strategy. The National Defense Strategy is then used to establish the plans for military force structure, force modernization, business processes, supporting infrastructure, and required resources (funding and manpower). The QDR final report is provided to Congress in the second year of the administration. In the PPBE process, the QDR final report serves as the foundation document for defense strategy and business policy. Since this document is not available until the second year, the first year of the administration is treated as an off-year, using the President's Budget inherited from the previous administration as a baseline. In the second year, which is treated as an on-year, the Guidance for the Development of the Force and Joint Programming Guidance are rewritten to implement the QDR of the new administration.

1.3. Joint Capabilities Integration and Development System (JCIDS)

JCIDS plays a key role in identifying the capabilities required by the warfighters to support the National Security Strategy and the National Defense Strategy. Successful delivery of those capabilities relies on the JCIDS process working in concert with other joint and DOD decision processes. JCIDS procedures support the Chairman and Joint Requirements Oversight Council (JROC) in advising the Secretary of Defense on identifying and assessing joint military capability needs. JCIDS is a joint-concepts-centric capabilities identification process that allows joint forces to meet future military challenges. The JCIDS process assesses existing and proposed capabilities in light of their contribution to future joint concepts. The JCIDS process was created to support the statutory requirements of the JROC to validate joint warfighting requirements. JCIDS is also a key supporting process for the DOD acquisition and Planning, Programming, and Budget Execution (PPBE) processes. The primary objective of the JCIDS process is to ensure the capabilities required by the joint warfighter to successfully execute the missions assigned to them are identified with their associated operational performance criteria. This is done through an open process that provides the JROC the information they need to make decisions on required capabilities. The requirements process supports the acquisition process by providing validated capability needs and associated performance criteria to be used as a basis for acquiring the right weapon systems. Additionally, JCIDS provides the PPBE process with affordability advice supported by the capabilities-based assessment (CBA), and identifies capability gaps and potential materiel and non-materiel solutions. While it considers the full range of doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) solutions, for purposes of this Guidebook, the focus is on the pursuit of "materiel" solutions.

JCIDS acknowledges the need to project and sustain joint forces and to conduct flexible, distributed, and highly-networked operations. JCIDS is consistent with DoD Directive 5000.01 direction for early and continuous collaboration throughout the Department of Defense. JCIDS implements a capabilities-based approach that leverages the expertise of government agencies, industry, and academia. JCIDS encourages collaboration between operators and materiel providers early in the process. JCIDS defines interoperable, joint capabilities that will best meet the future needs. The broader DoD acquisition community must then deliver these technologically sound, sustainable, and affordable increments of militarily useful capability to the warfighters.

JCIDS informs the acquisition process by identifying and assessing joint military capability needs which need a materiel solution; these identified capability needs then serve as the basis for the development and production of acquisition programs. JCIDS is fully described in CJCS Instruction 3170.01, signed by the Chairman of the Joint Chiefs of Staff. This instruction establishes the policies for JCIDS, and provides a top-level description of the process. A supplementary manual, the JCIDS Manual, provides the details necessary for the day-to-day work in identifying, describing, and justifying joint warfighting capabilities. The manual also includes the formats that describe the content required for each JCIDS document.

For major defense acquisition programs or major automated information systems subject to OSD oversight, the products of the Joint Capabilities Integration and Development System process

directly support the Defense Acquisition Board (DAB) and Information Technology Acquisition Board (ITAB) in advising the Milestone Decision Authority for major milestone decisions. Figure 1.3.F1 is a simplified portrayal of the nature of this support. JCIDS provides similar support to other acquisition programs, regardless of the milestone decision authority. Where appropriate, the JCIDS process and its products may be tailored when applied to automated information systems.

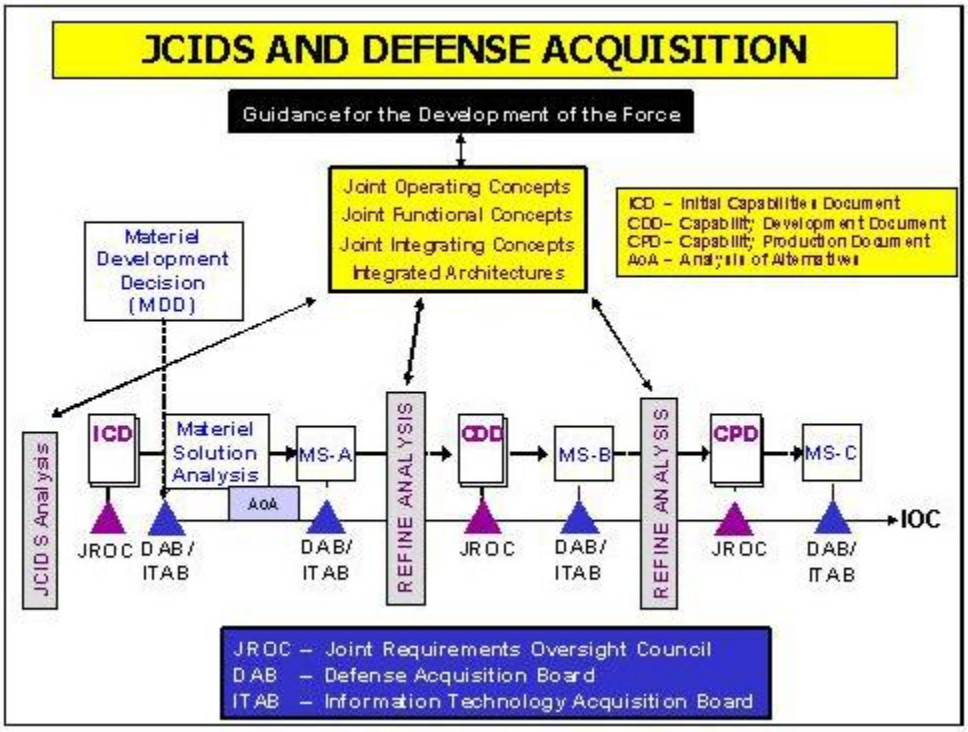


Figure 1.3.F1. JCIDS and Defense Acquisition

Figure 1.3.F1 depicts several key points. First, JCIDS is based on a series of top-down analyses ultimately derived from formal strategic-level guidance, including the National Security Strategy, National Defense Strategy, Joint Vision 2020, and the Report of the Quadrennial Defense Review. Second, these analyses assess existing and proposed capabilities in terms of their contribution to emerging joint warfighting concepts. Moreover, rather than focusing on the capabilities of individual weapon systems in isolation, the analyses assess capabilities in the context of integrated architectures of multiple interoperable systems. Third, from these overarching concepts, the JCIDS analysis process identifies capability gaps or shortcomings, and assesses the risks associated with these gaps. These gaps may be addressed by a combination of materiel and/or non-materiel solutions (non-materiel solutions would be changes to doctrine, organization, training, leadership and education, personnel, and facilities). Fourth, recommended materiel solutions, once approved, lead to acquisition programs. JCIDS documents are provided for these programs at each acquisition milestone and guide the subsequent development, production, and testing of the program. Further information on Capabilities-Based Assessment,

as well as the nature and role of the Initial Capabilities Document, Capability Development Document, and Capability Production Document can be found in the JCIDS Manual.

For Acquisition Category I and IA programs, and other programs designated as high-interest, the JROC reviews and validates all JCIDS documents under its purview. For Acquisition Category ID and IAM programs, the JROC makes recommendations to the DAB or ITAB, based on such reviews. Section 181 of title 10, United States Code, establishes JROC responsibilities. The Vice Chairman of the Joint Chiefs of Staff chairs the JROC, and is also a member of the DAB. The other JROC members are the Vice Chiefs of each military service. The "Expanded JROC" staff brings together key stakeholders from across the department and Interagencies, when appropriate, to shape decisions in support of the Joint warfighter. These stakeholders provide advisory support to the JROC.

Related Link: Capabilities-Based Assessment User's Guide

1.4. Defense Acquisition System

The Defense Acquisition System is the management process for all DoD acquisition programs. DoD Directive 5000.01, The Defense Acquisition System, provides the policies and principles that govern defense acquisition. DoD Instruction 5000.02, Operation of the Defense Acquisition System, establishes the management framework that implements these policies and principles. The Defense Acquisition Management System is an event-based process. Acquisition programs proceed through a series of milestone reviews and other decision points that may authorize entry into a significant new program phase. Details of the reviews, decision points, and program phases are found beginning with in paragraph 3 of Enclosure 2 of the Instruction. The Instruction also identifies the specific statutory and regulatory information requirements for each milestone and decision point.

One key principle of the defense acquisition system is the use of acquisition categories, where programs of increasing dollar value and management interest are subject to increasing levels of oversight. DoD Instruction 5000.02 Enclosure 3 identifies the specific dollar values and other thresholds for these acquisition categories. The most expensive programs are known as Major Defense Acquisition Programs (MDAPs) or Major Automated Information System (MAIS) programs. MDAPs and MAIS programs have the most extensive statutory and regulatory reporting requirements. Some elements of the defense acquisition system only apply to weapon systems, some element only apply to automated information systems, and some elements apply to both. DoD Instruction 5000.02, Enclosures 2, 3, and 4 provide specific details.

The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) is the Defense Acquisition Executive (DAE). The USD(AT&L) reviews ACAT ID programs and is the Milestone Decision Authority (MDA). A Defense Acquisition Board (DAB), chaired by the USD(AT&L), provides advice on critical acquisition decisions. DAB members are senior officials from the Joint Staff, the Military Departments, and staff offices within OSD.

The DAE may delegate decision authority for an MDAP to the DoD Component Head, who may, and generally will, delegate decision authority to the Component Acquisition Executive. Such delegation makes the program an ACAT IC program.

The DAE is also the MDA for MAIS programs that are ACAT IAM programs. An Information Technology Acquisition Board (ITAB) provides the DAE advice on critical acquisition decisions for ACAT IAM programs. The DAE may designate the ASD(NII) as the MDA for selected MAIS programs.

As with MDAPs, the DAE may delegate decision authority for an MAIS to the DoD Component Head, who may, and generally will, delegate decision authority to the Component Acquisition Executive. Such delegation makes the program an ACAT IAC program.

Both the DAB and the ITAB are further supported by a subordinate group in OSD known as an Overarching Integrated Product Team (OIPT). Each OIPT facilitates communication and vets issues before the DAB or ITAB meets. In this facilitator's role, the OIPT charters Working-level Integrated Product Teams for each review and manages their activities. At the Milestone Decision Review, the OIPT leader provides the DAB or ITAB members with an integrated assessment of program issues gathered through the Integrated Product Team process as well as various independent assessments.

DEFENSE ACQUISITION GUIDEBOOK
Chapter 2 -- Acquisition Program Baselines, Technology Development Strategies, and Acquisition Strategies

2.0. Overview

2.0.1. Purpose

The purpose of this Chapter is to provide program managers (PMs) the information and guidance needed to develop and maintain the Acquisition Program Baseline (APB), the Technology Development Strategy (TDS) and the Acquisition Strategy (AS) all required to effectively manage the program. The APB serves to document what the PM will deliver in terms of cost, schedule and performance. The TDS and AS describe the PM's plan to achieve the cost, schedule and performance goals and summarize the program planning and resulting program structure.

This Chapter will be updated as policy and statute evolve.

2.0.2. Contents

Section 2.1 describes the Acquisition Program Baseline. Section 2.2 discusses the Technology Development Strategy, and Section 2.3 discusses the Acquisition Strategy leading to the achievement of the program goals. Section 2.4 is a high level summary of some fundamental differences between an acquisition plan and an Acquisition Strategy.

2.0.3. Strategies and Plans

The Technology Development Strategy (TDS) and the Acquisition Strategy share many common required information elements, and each is the guiding strategy for the prospective phase of the Defense Acquisition Management System. The Acquisition Strategy and TDS should be forward looking and contain the key aspects of the program or pre-program efforts to execute the objectives of the phase, and the overall strategy to operational status. The TDS and Acquisition Strategy also include the detail for various plans, data and milestone information. The Acquisition Strategy and TDS must also satisfy statutory and regulatory information requirements for entry into the upcoming acquisition phase. The best strategy documents also distill the essence of managing the program or pre-program affordably, on schedule, and delivering the prescribed performance across the life cycle.

Both strategies guide the associated phase of acquisition and address the requirements supporting the development. Each increment should have its own program strategy document (AS or TDS), or minimally have a distinctly separate annex from the 'core' program strategy document. A strategy document annex for an increment can leverage the core program information when appropriate.

Acquisition Plan. Programs and pre-programs often combine the Acquisition Strategy (or TDS) and Acquisition Plan into a single document. An Acquisition Plan is a formal written document prepared by the Contracting Officer and the Program Manager (PM) reflecting the specific actions necessary to execute the approach established in the approved Acquisition Strategy and guiding contractual implementation, as referenced in Federal Acquisition Regulation (FAR) Subpart 7.1 and Defense Federal Acquisition Regulation Supplement (DFARS) Subpart 207.1. An Acquisition Plan does not require Milestone Decision Authority (MDA) approval and is not an Acquisition Strategy requirement, however the Plan may be included at the PM's discretion. See section 2.4 for further distinctions between an Acquisition Strategy and an Acquisition Plan, and section 2.3.10 Business Strategy for further procurement considerations.

TDS and Acquisition Strategy. The TDS and Acquisition Strategy content requirements have changed as a result of implementation of the Weapon Systems Acquisition Reform Act of 2009 (WSARA). The TDS is the pre-program strategy document preceding the Acquisition Strategy in most cases as pre-programs evolve into programs moving through the milestones in the acquisition management system. The TDS should serve as an information baseline for efforts that continually evolve during the progression through the acquisition management system assuming successful program initiation at Milestone B. The Acquisition Strategy content requirements vary according to program phase/milestone. For instance a Production and Deployment phase strategy will have a greater sustainment focus and include equipment valuation information that would not be included in an Engineering and Manufacturing Development phase Acquisition Strategy. Conversely, as the program progresses the Acquisition Strategy should reflect less technology maturation efforts as the technologies should be mature prior to production. A TDS or an Acquisition Strategy should be a forward looking document with only the minimum sufficient background information to facilitate understanding of the forward looking strategy.

Development of a TDS or Acquisition Strategy requires collaboration between the MDA, PM (or pre-program "PM"), their staffs, and the functional communities engaged in and supporting DoD acquisition throughout the full life cycle. A well-developed strategy optimizes the time and cost required to satisfy approved capability needs, and maximizes affordability throughout the program life cycle. The charge of DoD executive leadership is to use common sense and sound business practices in developing the Acquisition Strategy and executing the program. The PM should utilize Integrated Product and Process Development principles to assist in development of the strategy and execution of the program.

In this Chapter, the information elements for a TDS and an Acquisition Strategy are aligned by section to facilitate correlation for efforts that choose to use this Chapter as an initial strategy document 'template' (i.e., Section 2.2.xyz is for the widget schedule in a TDS, and Section 2.3.xyz is for the widget schedule in an Acquisition Strategy). There currently is no required format for a TDS or Acquisition Strategy, but the information headers (sub-section titles) are derived from source requirements, with OSD organizational considerations mixed in. Using the information headers from this Chapter can facilitate the review and approval process for TDS and AS documents.

TDS, Acquisition Strategy, Systems Engineering Plan (SEP), and Test and Evaluation Master Plan (TEMP). The Acquisition Strategy or TDS, SEP, and Test and Evaluation Strategy (TES) or TEMP should all align, with minimal overlap. The Acquisition Strategy or TDS should describe the integrated plans that identify the acquisition approach, and describes the business, developmental, and support strategies to manage program risks and meet program objectives while balancing cost, schedule and performance. The SEP should describe the technical planning and systems engineering processes that will be used to develop and manage the system and/or technical product development. The TES or TEMP should articulate how the technologies and system products will be tested to verify maturity and capability.

TDS and Acquisition Strategy Approval Process. An Acquisition Strategy or TDS requires the concurrence of the Program Executive Officer (PEO) (for programs in all acquisition categories) and the DoD Component Acquisition Executive (CAE) (for Acquisition Category (ACAT) ID and IAM programs) prior to approval by the MDA. MDA approval of the Strategy may precede a Milestone decision (e.g., to allow release of a Final Request for Proposals); however, programs may not proceed beyond a Milestone decision without an MDA-approved Strategy.

The efforts defined in the approved program strategy for a given phase of the acquisition management system (e.g. EMD) must align with efforts performed and included in the contract(s) for that phase. An AS that is approved for Milestone B approval should be consistent with efforts performed during the EMD phase, and be updated during that phase to reflect changes with the EMD strategy. An updated AS must be approved prior to Low Rate Initial Production (LRIP) and Full Rate Production (FRP) RFP release, but no later than the Milestone C or FRP decision by the MDA.

For ACAT ID anticipated programs the OSD entry point for a TDS or Acquisition Strategy is office of the Under Secretary of Defense for Acquisition, Technology and Logistics (OUSD (AT&L)) Acquisition Management; for ACAT IAM anticipated programs it is office of the Assistant Secretary of Defense for Networks and Information Integration (OASD (NII))/DoD Chief of Information Officer (CIO). Engagement with OSD regarding a TDS or an Acquisition Strategy to be approved by the DAE/MDA should begin not later than when the PM is ready to sign the document. For ACAT ID programs, pre-programs, or Special Interest programs with DAE oversight, documents will be coordinated across the OSD staff in both a Draft and a Formal round of coordination. The Formal coordination round is time driven and at the Senior Executive Service(SES)/General Officer/Flag Officer level and initiates only after the CAE signs the document; Draft coordination includes the non-SES-level work that precedes Formal coordination. More specifics about the coordination business rules will be in Chapter 10 when they are finalized.

Administrative. Acquisition Strategy and TDS documents need to be marked for proper handling. Classified documents, or classified Acquisition Strategy or TDS appendices, should be handled in the appropriate manners separate from the main unclassified Acquisition Strategy or TDS content. A TDS or Acquisition Strategy should be considered to be For Official Use Only (FOUO), marked appropriately, and handled as controlled unclassified information. Additionally if the document contains proprietary information or is competition sensitive it should be so marked.

In addition to FOUO and other appropriate markings, it is a good idea for a TDS or Acquisition Strategy to have a distribution statement. An example follows:

Distribution Statement – Distribution authorized to U.S. Government Agencies and their contractors; Other requests must be referred to [enter the cognizant PEO program office].Program Office), Address, City, State, Zip Code.

Programs that wish to use this Chapter as a template for their TDS or Acquisition Strategy should note that some fundamental elements such as an executive summary, signature page, overview or background, table of contents, acronym list, etc are not covered in this Chapter at this time. These requirements will be satisfied in each document.

2.1. Program Goals

2.1. Program Goals

Program goals are the measurable cost, schedule, and performance parameters necessary to describe program objectives. The most critical ones are articulated as Key Performance Parameters or Key System Attributes. The MDA should approve or define the cost, schedule and performance goals for Major Defense Acquisition Programs, and office of the Under Secretary of Defense (Comptroller) should evaluate the cost goals.

2.1.1. The Acquisition Program Baseline (APB)

DoD Instruction 5000.02 requires every program manager to propose and document program goals prior to, and for approval at, program initiation for all Acquisition Category (ACAT) programs. The APB satisfies the requirements in 10 USC 2435 and 10 USC 2220 for ACAT I Programs. The APB is an important document for program management and should reflect the approved program being executed.

A separate APB is required for each increment or sub-program of a major defense acquisition program (MDAP). Increments can be used to plan concurrent or sequential efforts to deliver capability more quickly and in line with the technological maturity of each increment. When an MDAP requires the delivery of two or more categories of end items that differ significantly in form and function, subprograms may be established.

Program goals consist of an objective value and a threshold value for each Key Performance Parameter (KPP)/Key System Attribute (KSA) parameter. Cost, schedule and performance are intrinsically linked and the threshold and objective values of all program goals should be developed with these relationships in mind. The program manager (PM) is responsible for managing the trade space between program goals within the bounds of cost, schedule and performance.

Objective values represent the desired operational goal associated with a performance attribute beyond which any gain in utility does not warrant additional expenditure. Generally, the objective value is an operationally significant increment above the threshold. An objective value may be the same as the threshold when an operationally significant increment above the threshold is not useful.

Thresholds represent the minimum acceptable operational value below which the utility of the system becomes questionable. For performance, a threshold represents either a minimum or maximum acceptable value, while for schedule and cost parameters, thresholds would normally represent maximum allowable values. The failure to attain program thresholds may degrade system performance, delay the program (possibly impacting related programs or systems), or

make the program too costly. The failure to attain program thresholds, therefore, places the overall affordability of the program and/or the capability provided by the system into question.

As noted above, each APB parameter must have both an objective and a threshold. For each performance parameter, if no objective is specified, the threshold value will serve as the objective value, and if no threshold is specified, the objective value will serve as the threshold value. For schedule and cost parameters, there are specified default threshold values: the default threshold for schedule is the objective value plus 6 months; and the default threshold for cost is the objective value plus ten percent of the objective value. Despite these guidelines, the PM may propose with justification an appropriate threshold value to optimize program trade space, subject to Milestone Decision Authority (MDA) and user approval.

The PM derives the APB from the users' performance requirements, schedule planning and requirements, and best estimates of total program cost consistent with projected funding. The sponsor of a capability needs document (i.e., Capability Development Document or Capability Production Document) provides a threshold and an objective value for each attribute that describes an aspect of a system or capability to be developed or acquired. The PM will use this information to develop an optimal product within the available trade space. APB parameter values should represent the program as it is expected to be developed, produced and/or deployed, sustained and funded.

Per 10 USC 2435, the Department of Defense (DoD) may not obligate funds for Major Defense Acquisition Programs after entry into Engineering and Manufacturing Development without an MDA-approved baseline unless the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) specifically approves the obligation. DoD Instruction 5000.02 extends this policy to ACAT IA programs. For an ACAT IA program, the Assistant Secretary of Defense for Networks and Information Integration must approve the obligation, unless the USD(AT&L) has retained oversight.

2.1.1.1. Acquisition Program Baseline (APB) Approval

The program manager (PM), in coordination with the user/sponsor, prepares the APB for program initiation. The PM can propose for approval a revision of the APB for each milestone review. The PM can also propose for approval a revision of the APB as a result of major program restructures that are fully funded and approved by the Milestone Decision Authority (MDA), or as a result of program deviations (breaches), if the breach is primarily the result of external causes beyond the control of the PM and approved by the MDA.

The MDA is the approval authority for the APB. The APB requires the concurrence of the Program Executive Officer for all Acquisition Category (ACAT) programs, and the concurrence of the DoD Component Acquisition Executive for ACAT ID and IAM programs.

For ACAT I and IA programs and Joint Requirements Oversight Council Interest Programs, the APB will be coordinated with the appropriate Department stakeholders, minimally including

Defense Acquisition Board or Information Technology Acquisition Board members and advisors, prior to MDA approval.

2.1.1.2. Trade-Offs

Maximizing program manager (PM) and contractor flexibility to make cost/performance trade-offs is essential to achieving cost objectives. The PM may treat the difference between an objective and its associated threshold as trade space if the combination values lie within the established thresholds and objectives. Additionally as development trade space is exercised the impacts between cost, schedule and performance should be understood and considered so that values remain within their established thresholds and objectives.

The best time to reduce total ownership cost and program schedule is early in the acquisition process. Continuous cost/schedule/performance trade-off analyses can help attain cost and schedule reductions.

Cost, schedule, and performance may be traded within the "trade space" between the objective and the threshold without obtaining Milestone Decision Authority (MDA) approval. Making trade-offs outside the trade space (i.e., decisions that result in acquisition program parameter changes) require approval of both the MDA and the capability needs approval authority. Validated Key Performance Parameters may not be traded-off without approval by the validation authority. The PM and the user should work together on all trade-off decisions.

In 2007, the requirement to form configuration steering boards (CSBs) was established. CSBs are a core part of managing the cost, schedule, and performance trade space for acquisition programs. Annual (minimally) CSBs are to be held to review all requirements changes and any significant technical configuration changes for Acquisition Category (ACAT) I and IA programs in development that have the potential to result in cost and schedule impacts to the program. Such changes will generally be rejected, deferring them to future blocks or increments. Changes are not to be approved unless funds are identified and schedule impacts mitigated. The PM, in consultation with the Program Executive Officer, shall, on a roughly annual basis, identify and propose a set of de-scope options, with supporting rationale addressing operational implications, to the CSB that reduce program cost or moderate requirements. The CSB shall recommend to the MDA (if an ACAT ID or IAM program) which of these options should be implemented. Final decisions on de-scope option implementation shall be coordinated with the Joint Staff and military department requirements officials.

2.1.1.3. Acquisition Program Baseline (APB) Management

The program manager (PM) should immediately notify the Milestone Decision Authority (MDA) via a Program Deviation Report when the PM's current estimate exceeds one or more APB threshold values for cost, schedule, and/or performance. Only the MDA can approve a revision to the APB. Before undertaking revisions to a MDAP APB, consultation with office of the Under Secretary of Defense for Acquisition, Technology and Logistics (OUSD(AT&L)), Office of

Acquisition Resources and Analysis (ARA) and the Overarching Integrated Product Team leader is recommended. For a Major Automated Information System (MAIS) program, consultation with the office of the Assistant Secretary of Defense for Networks and Information Integration (OASD(NII)), Office of Deputy to the ASD(NII) for Command, Control, Communications, Intelligence, Surveillance and Reconnaissance and Information Technology Acquisition is recommended, unless the USD(AT&L) has retained authority for the program.

For MDAPs, both "original" and current APBs are maintained. The original APB cost estimate may be revised only if a breach occurs that exceeds the critical cost growth threshold for the program. The "critical" cost growth threshold, as it relates to the original APB, is defined to be an increase of at least 50 percent over the original Program Acquisition Unit Cost (PAUC) or the original Average Procurement Unit Cost (APUC) for the program. The "critical" cost growth threshold, as it relates to the current APB, is defined to be an increase of at least 25 percent over the current PAUC or APUC for the MDAP.

For MAIS programs, only a current APB is maintained, but the baseline reported in the MAIS Annual Report (MAR) serves a similar purpose as an original APB baseline. (The MAR baseline—separate from the APB baseline—can be revised only after a Critical Change Process is completed. MAIS Critical Change thresholds are: cost parameter increase greater than 25%, schedule parameter delay greater than 12 months, or failure to meet a key performance parameter.)

For both MDAP and MAIS programs, the current APB shall be revised at Milestone decisions, and at the full-rate production decision (full deployment decisions for MAIS). Other than these occasions, current APBs may be revised only as a result of major program restructures that are fully funded and approved by the MDA, or as a result of program deviations (breaches), if the breach is primarily the result of external causes beyond the control of the PM. Multiple revisions to the current APB, however, will not be authorized, and in no event will a revision to the current APB be authorized if it is proposed merely to avoid a reportable breach. The determination of whether to revise the APB will be made by the MDA.

For MDAPs, a "critical" cost growth breach triggers the title 10 USC 2433 ("Nunn-McCurdy") certification process. In that case, both the current and original APBs shall be revised to reflect the same new APB values, assuming the program is certified. For MAIS programs, a Critical Change triggers the similar process implementing title 10 USC 2445c.

2.1.1.4. Acquisition Program Baseline (APB) Content

The APB is an important management document which articulates the approved program's objective and threshold boundaries, and links cost, schedule and performance parameters. The program manager (PM) manages the program within that trade space.

Cost. Cost figures should reflect realistic cost estimates of the total program and/or increment. Budgeted amounts should never exceed the total cost thresholds (i.e., maximum costs) in the

APB. As the program progresses, the PM can refine procurement costs based on contractor actual (return) costs from Technology Development, Integrated System Design, System Capability and Manufacturing Process Demonstration, and Low-Rate Initial Production.

The cost parameters of Acquisition Category (ACAT) IA programs are the same as those for ACAT I programs as noted in the next paragraph with the addition of military pay and the cost of acquisition items procured with Defense Working Capital Funds.

The APB should contain cost parameters (objectives and thresholds) for major elements of program life-cycle costs (or total ownership costs), as defined in Section 3.1. These elements include:

1. Research, development, test, and evaluation costs
2. Procurement costs (including the logistics cost elements required to implement the approved sustainment strategy)
3. Military construction costs
4. Operations and maintenance (O&M) costs (that support the production and deployment phase, as well as acquisition related (O&M)) if any
5. Total system quantity (to include both fully configured development and production units)
6. Average Procurement Unit Cost defined as total procurement cost divided by total procurement quantity (Note: This item and item 7 below do not usually apply to business information technology systems or other software-intensive systems with no production components)
7. Program Acquisition Unit Cost defined as the total of all acquisition-related appropriations divided by the total quantity of fully configured end items
8. Any other cost objectives established by the Milestone Decision Authority (e.g. Ownership cost)

The cost parameters are presented in both base year and then year dollars. The threshold parameters for cost are only presented in base year dollars.

Schedule. Schedule parameters should include, as a minimum, the projected dates for program initiation, other major decision points (such as other milestones and the system-level Preliminary Design Review and Critical Design Review), major testing events, and Initial Operational Capability (IOC). To be consistent with 10 USC 144A, Major Automated Information System programs schedule parameters should include Milestone A, Milestone B, Milestone C, Full Deployment, IOC, and Full Operational Capability, depending on where the program enters the acquisition process. The Capability Development Document (CDD) and Capability Production Document (CPD) program summaries describe the overall program strategy for reaching full capability, and the timing of the delivery of each increment. The PM may propose, and the MDA may approve, other, specific, critical, and system events.

Performance. The total number of performance parameters should be the minimum number needed to characterize the major drivers of operational performance. Performance parameters should include the key performance parameters identified in the capability needs document(s) (i.e., CDD and CPD), and the values and meanings of thresholds and objectives should be consistent. (See also CJCS Instruction 3170.01G.) The number and specificity of performance parameters may change over time. Early in a program, the APB should reflect broadly defined, operational-level measures of effectiveness or measures of performance to describe needed capabilities. As a program matures, system-level requirements become better defined. The MDA may also add performance parameters to the APB other than the Joint Requirements Oversight Council (JROC)-validated Key Performance Parameters.

OSD will review and comment on APBs for ACAT ID, Special Interest programs, and other programs designated by the Defense Acquisition Executive. The Joint Staff (J-8) will review the cost, schedule, and key performance parameter objective and threshold values in the APB for JROC Interest programs, and any other programs of significant joint interest (as determined by the J-8). The J-8 review will ensure that the objective and threshold values are consistent with the JROC-approved CDD, the CPD, and prior JROC decision(s). The review will also ensure that the baseline provides the necessary warfighting capabilities affordably and within required time frames. (See also CJCS Instruction 3170.01.)

2.1.1.5. Acquisition Program Baseline (APB) for an Evolutionary Acquisition Program

Evolutionary acquisition is the preferred DoD strategy for rapid acquisition of mature technology for the user. An evolutionary approach delivers capability in militarily useful increments, recognizing, up front, the need for future capability improvements.

Programs using an evolutionary acquisition strategy should design the APB consistent with the sponsor's capability document(s) and the applicable example approaches outlined in Table 2.1.1.5.T1.

CDD or CPD	APB
Capability Development Document (CDD) defines multiple increments of capability	APB contains multiple sets of parameter values, each set defining an increment
A separate CDD for each increment	A separate APB for each increment
There is one Capability Production Document (CPD) for each production increment	The corresponding APB should be updated to reflect the parameters in the CPD for that production increment

Table 2.1.1.5.T1. APB Parameters under an Evolutionary Acquisition Strategy.

DoD Instruction 5000.02 requires the Milestone Decision Authority (MDA) to formally initiate each increment of an evolutionary acquisition program. Program initiation may occur at Milestone B or C. Therefore, the program manager should develop APB documented goals for each program increment or sub-program. Each increment will have its own set of threshold and objective values set by the user. Block upgrades, pre-planned product improvement, and similar efforts that provide a significant increase in operational capability and meet an acquisition category threshold specified in this document shall be managed as separate increments.

The Fiscal Year 2009 National Defense Authorization Act added a new section to title 10 (section 2430a) that permits the Secretary of Defense (delegated to the Under Secretary of Defense for Acquisition, Technology and Logistics) to designate subprograms within a Major Defense Acquisition Program (MDAP). That is, when an MDAP requires the delivery of two or more categories of end items that differ significantly in form and function, subprograms may be established for baseline development and reporting purposes. The law stipulates that when one subprogram is designated within an MDAP, all remaining elements (increments or components) of the program shall also be appropriately organized into one or more other subprograms.

The decision whether to establish subprograms for an MDAP requires careful analysis and must be made on a case-by-case basis. Structuring an MDAP with subprograms should reflect the way the program is being managed, and represent the most efficient and informative way to convey information about a program to senior defense acquisition officials as well as to the Congress.

The law requires that the congressional defense committees be notified in writing of any proposed subprogram designation not less than 30 days before the date such designation takes effect. The approval of an APB reflecting such designation will be considered the date that subprogram designation takes effect; therefore, notification to Congress must occur not less than 30 days before a subprogram APB is approved. Accordingly, DoD Components must notify the Director, Acquisition Resources and Analysis of all proposed APBs that reflect new or revised subprogram designation at least 60 days before the proposed APB is submitted to the MDA for approval.

2.2. Pre-Systems Acquisition: Technology Development Strategy (TDS)

The Defense Acquisition Management System incorporates a Technology Development (TD) Phase subsequent to the Materiel Solution Analysis Phase. The purpose of the TD Phase is to reduce technology risk, determine the appropriate set of technologies to be integrated into a full system, demonstrate critical technologies on representative prototypes, and in many cases to initiate traceable requirements flow down to complete a preliminary design for the full requirement/full system.

DoD Instruction 5000.02 requires a Milestone Decision Authority (MDA)-approved TDS for each increment of an evolutionary acquisition program that includes a Milestone A (a TD Phase). It suggests that multiple TD demonstrations may be necessary before the user and developer

agree that a proposed technology solution is affordable, militarily useful, and based on mature technology.

The TDS should guide efforts through the TD Phase within the established cost goals. The TD Phase may be planned to include the System Requirements Review (SRR), System Functional Review (SFR), and Preliminary Design Review (PDR), which begs a level of maturity in a capabilities document, specifically a Capability Development Document (CDD). The CDD is a Milestone B requirement, so program or project offices planning a PDR in the TD Phase need to work closely with the requirements and capabilities communities to integrate development schedules. The TD Phase begins based on the Analysis of Alternatives (AoA) results and an Initial Capabilities Document (ICD) that may be at a very high level. If full system SRR and SFR activities are planned in the TD Phase they should depend on a stable, draft, CDD or run the risk of not having traceable lower level requirements at the PDR. Programs in the TD Phase should employ competitive prototyping to the maximum extent possible, where resources permit. Competitive prototyping is discussed in section 2.2.8.2.

The TDS should ensure appropriate efforts are undertaken to meet the statutory Milestone B certification criteria as well as regulatory requirements for entry into the Engineering and Manufacturing Development phase. Final Requests for Proposals for a TD Phase cannot be released, nor any action be taken that would commit the pre-program to a particular contracting strategy, until the MDA has approved the TDS.

The TDS must be approved for entry into the TD Phase, and precedes the formal Acquisition Strategy unless program initiation is at Milestone A (currently a potential exception for shipbuilding programs only). The TDS is not a requirement at Milestone B and beyond, but a technology maturation plan/strategy should be part of the Engineering and Manufacturing Development Phase Acquisition Strategy for those elements that require additional concurrency and technological development to achieve the next level of maturity (e.g., Technology Readiness Level (TRL) 7 at Critical Design Review or Milestone C). If the Acquisition Strategy is approved at Milestone A, the TDS content should be included as part of the Acquisition Strategy.

The project can exit TD when an affordable program or increment of militarily-useful capability has been identified, the technology and manufacturing processes for that program or increment have been assessed and demonstrated in a relevant environment and found to be sufficiently mature, manufacturing risks have been identified and assessed, and a system or increment can be developed for production within a short timeframe (normally less than 5 years); or, when the MDA decides to terminate the effort. If the requirement for a PDR was approved in the TDS for this phase it must have been successfully conducted, in accordance with the SRR and SFR. Entry criteria for the Engineering and Manufacturing Development Phase must be met for a Milestone B approval.

The following content is appropriate for a TDS.

The TDS should focus on the activities of the TD Phase, including maturation efforts to achieve at least TRL 6, as well as overall project maturation to Initial Operational Capability to ensure a program can be defined with reasonable risk to meet cost, schedule and performance goals. The TD Phase should be planned to go beyond pure technology development and include a full system PDR. The requirements translation and development and design efforts sufficient to complete the PDR should be briefly summarized in the TDS

The TDS should generally discuss activities associated with the subsequent phases of the planned acquisition, and include a top level schedule projecting major events into the Operations and Support phase. If the strategy described in the TDS will limit the opportunities for competitive procurement in any phase of the acquisition framework, the TDS should identify and justify those limitations. The TDS for the TD Phase is analogous to the Acquisition Strategy for subsequent phases.

2.2.1. Acquisition Approach

2.2.1.1. Open Systems Strategy Summary

2.2.1.2. Tailoring

2.2.1. Acquisition Approach

The Technology Development Strategy (TDS) should include a discussion of the planned acquisition approach to manage research and development, including a summary of the considerations and rationale supporting the chosen approach and a preliminary description of how the post-Milestone B program may be envisioned to be divided into technology and/or capability development increments. Whether the acquisition approach is evolutionary or single step to full capability should be discretely defined and justified.

The acquisition approach section of the TDS is the appropriate place for a strategic discussion of the anticipated cost, schedule and performance drivers of the Technology Development (TD) Phase.

PDR planning should be discussed in the TDS for approval by the MDA at Milestone A. Detailed technical planning (e.g. technical performance metrics or PDR checklists) of the PDR are inappropriate for the TDS, but summary discussion of the scheduling of the planned precedent technical reviews (e.g. SRR, SFR) and interactions with requirements definition and flow down efforts are appropriate.

The acquisition approach section of the TDS should also describe the plans to demonstrate at, or by, the PDR a balance among program requirements, technology demands, and cost considerations in the pre-program. Additionally for shipbuilding programs, the TDS should describe plans to maintain contact with prospective shipbuilders, and other key industrial entities, to analyze cost and requirements trade-offs, and to identify ways to reduce the technical demands

of the ship as requirements evolve. These trade-offs should be performed within the bounds of cost, schedule and performance,. Additionally the DFARs must be observed.

The TDS should include proposed exit criteria for the TD Phase, and plans to support the entry criteria for the ensuing phase, presumably Engineering and Manufacturing Development. The TD Phase can be complete when an affordable program or increment of militarily useful capability has been identified; the technology and manufacturing processes for that program or increment have been assessed and demonstrated in a relevant environment; manufacturing risks have been identified; and a system or increment can be developed for production within a short timeframe.

Factors to consider, and to be expounded on separately in the technology maturation and schedule segments of the TDS include recognition of technology development and maturity, and if applicable, a System Requirements Review (SRR) and functional allocation and functional baseline, competitive prototyping strategy, and the Preliminary Design Review (PDR) approach.

2.2.1.1. Open Systems Strategy Summary

The summary of open system planning should describe how modular open systems architecture Modular Open Systems Approach (MOSA) will be employed in development. A more detailed description of open system planning may be appropriate in the Systems Engineering Plan. If upon completing a business case analysis, the program manager (PM) decides to acquire a system with closed interfaces, the PM should report to the Milestone Decision Authority, in context of the Acquisition Strategy, the justification for the decision. The justification should describe the potential impacts on the ability to access latest technologies from competitive sources of supply throughout the system life cycle, integrate the system with other systems in a joint integrated architecture venue, and to integrate and/or retrofit earlier increments with later increments in an evolutionary acquisition context.

The open systems strategy summary in the Technology Development Strategy, or Acquisition Strategy, should include a clear declaration of whether or not an open systems approach is planned, and a justification is required if the plan is for a closed systems approach.

2.2.1.2. Tailoring

The Technology Development Strategy (TDS) information contents and the application of the Defense Acquisition Management System to a pre-program effort can be tailored with the appropriate level of approval. Most statutory requirements either cannot be tailored or require Congressional approval to be omitted, so statutory tailoring is rare at best. Regulatory tailoring can be done with the approval of the Milestone Decision Authority (MDA), generally via an Acquisition Decision Memorandum (ADM), and/or in this section of the TDS if approval timing is appropriate.

The tailoring section of the TDS should contain proposed tailoring initiatives for MDA approval, as well as already approved (e.g. via ADM) tailoring plans and be complemented by rationale for why the policies, regulations or directives being proposed to be tailored are not relevant.

If no tailoring of Department policy is being proposed, it should be so stated.

- Note that 10USC 2366b requires the MDA to certify, prior to Milestone B approval, that the program complies with all relevant policies, regulations and directives of the Department of Defense.

2.2.2. Source and Related Documents

The Technology Development Strategy (TDS) should cite key source documents, such as and as a minimum, include:

- The underpinning approved capability document(s) (e.g,. Initial Capabilities Document) with a brief summary of the capability the acquisition is intended to provide
- The most recent Analysis of Alternatives (AoA)
- Any relevant or recent Acquisition Decision Memoranda

This section of the TDS should also cite complementary and concurrent documents such as the Test and Evaluation Strategy and Systems Engineering Plan.

Each citation should include the approval date and note the approval status. If a document is still in draft and not approved, it should be so noted and the projected approval date provided.

2.2.3. Capability Needs

To provide context, the Technology Development Strategy (TDS) should contain a summary description of the capability the acquisition is intended to satisfy or provide. The summary should highlight system characteristics driven by sustainment, by operational suitability, interoperability and/or joint integrated architectures, capability areas, and family or system of systems.

The source capability document for the Technology Development (TD) Phase will generally be an Initial Capabilities Document (ICD). If the ICD is very broad, such as those that can spawn a number of materiel solutions in separate programmatic efforts, the TDS should describe the subset of ICD requirements that the planned TD Phase will address.

Additionally, if a draft Capability Development Document (CDD) is anticipated to support a full system Preliminary Design Review PDR during the TD Phase it should be so noted. If a component, sub-system, partial system, or less capable prototype approach to the PDR is planned it should be accordingly noted, and a subsequent fully capable PDR should be planned. Regardless of the approach, the PDR and the System Requirements Review and System

Functional Review should be planned accordingly and reflected in the top-level integrated schedule.

The Life-cycle Signature Support Plan (LSSP) TDS content requirements are described in DAG section 2.2.16 and should ideally be included in/with the Capability Needs section of the TDS.

2.2.4. Top-Level Integrated Schedule

The Technology Development Strategy (TDS) should include a top-level integrated program schedule. It is generally best to use two schedule diagrams and they should be accompanied by expounding text and an acronym key.

A schedule diagram should reflect notional planning to Initial Operational Capability (IOC), and be noted as notional. The schedule diagram from "Milestone A to IOC" is ideally a separate diagram from the Technology Development (TD) Phase diagram that reflects "Materiel Development Decision (MDD) to Milestone B".

The forward planning Milestone A TD Phase integrated schedule should look backward in time to a few key events, and minimally include a diagram that notes when the Initial Capabilities Document, the Analysis of Alternatives (AoA), and the Alternative Systems Review were approved and/or completed.

The TD Phase schedule should note when the program manager (PM) proposes to undergo a Milestone A decision review to enter the TD Phase as well as key events designed to satisfy the requirements necessary to enter the next phase of development.

The TD Phase schedule should minimally identify technology demonstration and competitive prototyping activities, the planned technical reviews, and major contracting events including the proposed Engineering and Manufacturing Development contract Request for Proposal.

Planned technical reviews prior to a Milestone B decision should also be shown (e.g., Systems System Requirements Review , a System Functional Review , and program level Preliminary Design Review(s) (PDRs) , if applicable).

Whether the full-system PDR, traceable to a Capability Development Document (CDD) or stable, draft, CDD, is planned before or after Milestone B should be clear, and the rationale for that scheduling should be included in the text of this section.

2.2.5. Program Interdependency and Interoperability Summary

The summary should identify any dependency on the planned or existing capability of other programs or systems, including current or planned dependencies and connectivity with non-DoD programs (e.g., allied, friendly foreign or non-DoD agency).

A notional example would be for an air-launched missile materiel solution project in the Technology Development Phase to cite the aircraft programs that are expected to carry it (both U.S. and allied aircraft), as well as citing the seeker and warhead efforts that rely on two other weapons development programs that are on-going, including one which is underway by a closely allied nation.

2.2.5. Program Interdependency and Interoperability Summary

The program's Net-Centric Data Strategy approach should be summarized in the TDS. A more detailed approach will be required in the Information Support Plan (ISP) for subsequent milestone decisions.

2.2.6. International Cooperation

The PM should include a discussion of the international cooperative strategy sufficient to satisfy the statutory (10 USC 2350a) requirement for a Cooperative Opportunities document. In addition, DoD Directive 5000.01 requires coalition interoperability from DoD systems, units and forces. Complete details on International Cooperation requirements in DoD acquisitions in provided in Chapter 11, International Cooperation.

To streamline the required documentation for acquisition programs, AT&L has developed a template for a coalition interoperability section of Technology Development Strategies that includes the cooperative opportunities document requirement for 10 USC 2350a.

Considerations required are:

- a statement indicating whether or not a project similar to the one under consideration by the DoD is in development or production by any NATO country, Major Non-NATO Ally, or friendly foreign country.
- if a project similar to the one under consideration by the DoD is in development or production by any NATO country, Major Non-NATO Ally, or friendly foreign country, an assessment is to be provided by the PM for the USD(AT&L) as to whether that project could satisfy, or could be modified in scope so as to satisfy, the military requirements of the project of the United States under consideration by the DoD
- an assessment of the advantages and disadvantages with regard to program timing, developmental and life-cycle costs, technology sharing, and Rationalization, Standardization, and Interoperability (RSI) of seeking to structure a cooperative development program any NATO country, Major Non-NATO Ally, or friendly foreign country.
- the recommendation as to whether the DoD should explore the feasibility and desirability of a cooperative development program with one or more countries and any NATO country, Major Non-NATO Ally, or friendly foreign country.

The International Cooperation section of the Technology Development Strategy should address the PM's plan to meet the warfighter's requirements and to increase the opportunity for coalition interoperability as part of the developing DoD program.

Alternatives examined should include:

- existing defense programs and materiel from foreign sources that meet US requirements or can be modified to meet US requirements
- existing NATO or commercial standards that promote interoperable systems
- considerations for future use of system with coalition partners in operations
- opportunities for reciprocal defense trade and cooperation
- new cooperative research, development, test and evaluation projects with allied and partner nations to reduce U.S. costs and risk, and improve coalition capabilities of U.S. and partner systems
- shared production and logistics support in order to strengthen alliances and partnerships with NATO allies, non-NATO allies, and strategic partners
- interface and security requirements to support foreign military sales, or direct commercial sales of U.S. system

PMs have a responsibility to look across the breadth of the program to understand the numerous opportunities to engage the international community to the benefit of the United States, consistent with information security and technology transfer limitations.

To assist with the assessment, PMs should coordinate with their respective international programs offices to gain insight into international activities which may impact their program. This process should continue throughout the life cycle of the program and begin to reap tangible outcomes as the program progresses towards completion.

The detailed requirements are discussed in the Coalition Interoperability Template.

2.2.7. Risk and Risk Management

The program manager (PM) should establish a risk management process consistent with guidance in Guidebook Chapter 4, and summarize the process in the Technology Development Strategy (TDS).

The PM should summarize the program's key risks and include the related risk cube. The risk cube format should be taken from the Risk Management Guide for DoD Acquisition, 6th Edition, Version 1, dated August 2006. The TDS should describe how funding, schedule and performance are planned to be balanced and traded to manage/mitigate key risks.

The TDS should describe how the government will work with the contractor to ensure understanding of the technical requirements prior to MS B (prior to a detail design contract

award for ship programs). The government, while in a competitive environment, should ensure that the prospective contractors understand the technical specifications.

This section of the TDS should also include a brief description of the TD phase approach to retire risk and close any remaining gaps in design requirements prior to MS B approval and the award of an EMD phase contract. This risk reduction discussion should acknowledge the roles of technology maturation efforts and prototyping (section 2.2.8).

The TDS should refer to the Systems Engineering Plan for details on mitigation plans for the noted key Technology Development Phase risks, and to the program's Risk Management Plan for details on the risk management process.

2.2.8. Technology Maturation and Competitive Prototyping

2.2.8.1. Environment Definition

2.2.8.2. Competitive Prototyping

2.2.8. Technology Maturation

The Technology Maturation section of the TDS should include discussion of the identified preliminary critical technology elements (CTEs) and the respective strategies for attaining at least Technology Readiness Level (TRL) 6 prior to Milestone B should include the hardware, machinery, software, etc associated with the CTEs. For shipbuilding programs the TDS should describe plans for critical technologies to be developed into representative prototypes and achieve TRL 6 by the PDR.

Technology maturation efforts should be tied to programmatic (cost, schedule and performance) risk reduction and support a more accurate program cost for Milestone B and beyond.

While a TRA is not required for MS A approval, an early evaluation of technology maturity conducted shortly before MS A should be used to support the planning of technology development risk reduction efforts. See the TRA Deskbook.

Goals for maturation should be set with knowledge points established to assess maturity during the Technology Development Phase so that requirements analysis can be conducted. Time between testing and analysis should be allocated so that the user can assess this data along with other inputs to refine the Capability Development Document.

Key technical reviews, tests and/or demonstrations in the maturation of technology should be highlighted in the TDS. Details of the technical reviews and specific review criteria are more appropriate for the Systems Engineering Plan. Use of competitive prototyping should be considered as a tool for technology maturation and is discussed below.

A complete description of the technology demonstration strategy to support the capabilities identified in the Initial Capabilities Document and derived from the Analysis of Alternatives or other validated requirements should be included in the TDS. Additional test and evaluation information should be included in the Test and Evaluation Strategy. The TDS demonstration description should con

tain specific cost, schedule, and performance goals, including exit criteria, for the technology demonstration.

Before a contract is awarded for detail design of a new ship, critical technologies should be matured into actual system prototypes, or modeling and simulation if actual prototypes are impractical, and successfully demonstrated in a realistic environment.

2.2.8.1. Environment Definition

The acquisition project needs to relate the critical technology to a 'relevant environment' for the purposes of establishing Technology Readiness Level 6 ("System/subsystem model or prototype demonstration in a relevant environment") for that technology. Competitive Prototyping (see below) and other types of technology maturation need to consider the relevant environment in their planned development applications. The Technology Development Strategy should identify the relevant environment including potential threats against the capabilities desired and the physical environment (altitude, temperature, vibration, electro-magnetic, etc…), within which the materiel solution needs to operate. The characteristics of the environment should also be related to testing efforts in the Test and Evaluation Strategy.

2.2.8.2. Competitive Prototyping

The Technology Development Strategy (TDS) should include a description of the prototyping purpose and the prototyping strategy at the system and subsystem levels. The prototyping strategy should be competitive and provide for prototypes of the system or, if a system prototype is not feasible, for prototypes of critical subsystems before Milestone (MS) B approval. Information technology initiatives should prototype subsets of overall functionality, with the intention of reducing enterprise architecture risks, prioritizing functionality, and facilitating process re-design. These requirements can be waived only via a business case or national security justification and such a request for waiver should be discussed in the initial draft TDS.

The TDS should include the number of prototype units that may be produced and employed during the Technology Development phase. The description should also include a discussion of:

- How prototype units will be supported
- Specific performance goals and exit criteria that should be met by the employment of the prototypes

Prototyping is a tool for risk reduction; technology maturation; identifying and resolving integration risks; controlling manufacturing and sustainability risks, and minimizing risks of cost growth due to unknowns in design, assembly and integration. Competition provides opportunity for cost reduction and innovation, and is a mandatory consideration in Defense Acquisition. Competition is useful for addressing programmatic challenges such as cost growth in a sole source environment; responsiveness to program office direction; and can be used to strengthen the Government's bargaining position on data rights, per unit cost, and "in scope" determinations, etc. Also see section 2.3.10.4.

Competitive prototyping should be considered a key factor in the TDS and the Acquisition Strategy as well as a major vehicle for reducing technical risk. Competitive prototyping can:

- provide the source selection activities and the program manager (PM) with increased understanding of the technologies and technical approaches employed by competitors
- ensure the technologies and designs are suitable to satisfy program requirements
- provide development teams with the necessary hands-on experience with technologies and designs
- increase industry's motivation to provide a sound technical approach at a more affordable cost

Planned competitive prototyping is unique to each project. The PM can explore alternate concepts and innovations through competitive prototyping.

Government and industry teams should work together to demonstrate key knowledge elements that can inform future development and budget decisions. DoD Instruction 5000.02 requires two or more competing teams producing prototypes prior to Milestone B approval. Competitive prototyping of systems or key elements of systems will reduce technical and operational risk, validate designs and cost estimates, evaluate manufacturing processes, and help refine requirements. Knowing the purpose of the planned prototyping is important for initiating an effective program and for defining (and controlling) requirements. Focusing early in the TDS and Acquisition Strategy planning on the critical project risk items is important. Identifying the major risk items is critical in identifying what should be prototyped. Maintaining and utilizing past best practice methodologies in prototyping assists the PM in gaining better insight into the keys for a successful development and manufacturing program.

2.2.9. Industrial Capability and Manufacturing Capabilities

2.2.9.1. Industrial and Manufacturing Readiness

2.2.9. Industrial Capability and Manufacturing Capabilities

The Technology Development Strategy (TDS) should identify and address how industrial capabilities, including manufacturing technologies and capabilities, will be considered and matured during the Technology Development (TD) Phase. Industrial capabilities encompass

public and private capabilities to design, develop, manufacture, maintain, and manage DoD products.

A discussion of these considerations is needed to ensure the manufacturing capability will be assessed adequately, and reliable, cost-effective, and sufficient industrial capabilities will exist to support the program's overall cost, schedule, and performance goals for the total research and development program.

During the TD Phase the program office should conduct an industrial capabilities assessment. The resulting Industrial Base Capabilities Considerations will be summarized in the AS in support of Milestone B. The industrial capabilities assessment will address implications of the TDS for (1) a competitive marketplace; (2) the viability of any associated essential industrial/technological capabilities; and (3) the potential viability of non-selected firms as enduring competitors for defense products. In addressing these factors, consider:

- span of time between current and potential future contract awards that make selection critical to supplier business decisions
- other businesses of the same type or emerging capabilities that could serve as a replacement solution
- decisions that will impact a supplier's future viability (jeopardize future competitiveness or does not provide a sufficient business case to keep the capabilities/unit around for the future)
- decisions that will establish new industrial capabilities (new facilities, demonstrate and "productionize" new technologies, preserve health of the industrial base)

During the Materiel Solution Analysis Phase, the industrial and manufacturing capability should have been assessed for each competing alternative in the AoA. The results of the assessment should be used to develop the TDS by illustrating the differences between alternative approaches based on industrial and manufacturing resources needed.

2.2.9.1. Industrial and Manufacturing Readiness

The Technology Development Strategy (TDS) should summarize plans for how the industrial and manufacturing readiness will be addressed in the Technology Development (TD) Phase to ensure that manufacturing maturity is appropriate to enter Engineering and Manufacturing Development, particularly for new or high risk manufacturing endeavors.

During the TD Phase, the industrial and manufacturing capability should be assessed in light of each prototype and/or competing design under consideration. The purpose of this assessment is to baseline needed industrial capability and to identify remaining required investments. While it is not expected that contractors would have a complete factory and supply chain established this early in a program, key knowledge must be obtained on critical manufacturing processes, production scale-up efforts, and potential supply chain issues. TD Phase considerations should include:

- manufacturing processes and techniques not currently available
- design producibility risks
- probability of meeting delivery dates
- potential impact of critical and long-lead time material
- production equipment availability
- production unit cost goal realism
- cost and production schedule estimates to support management reviews
- manufacturing feasibility and cost and schedule impact analyses to support trade-offs among alternatives
- recommendations for anticipated production testing and demonstration efforts
- methods for conserving critical and strategic materials and mitigating supply disruption risks and program impacts associated with those materials

The Analysis of Alternatives (AoA), or efforts in the Materiel Solution Analysis Phase, should have identified new or high risk manufacturing capability or capacity risks if they exist. The TDS should highlight how these risks areas are going to be addressed and minimized in the TD Phase, on the path to full manufacturing capability in the Production and Deployment Phase. Specifically, where new or high risk manufacturing capability is forecasted the TDS should specify how this new capability will be demonstrated in a manufacturing environment relevant for the TD Phase. A TD Phase relevant environment is one that contains enough key elements of production realism (e.g. using manufacturing personnel or materials or equipment or tooling, or process steps, or work instructions, stated cycle time, etc.) to provide the pre-program adequate confidence that they would be able to execute the future program's cost, schedule and performance requirements, from a manufacturing perspective. The purpose of these demonstrations and analysis is to establish a baseline of needed industrial capabilities, and to identify the level of investments that will be required during Engineering and Manufacturing Development (EMD) when manufacturing readiness will grow toward production capability.

It is not expected that contractors would have a complete factory or supply chain established so early in a development effort, however, key knowledge should be obtained for new or high risk critical manufacturing processes, production scale-up efforts, and potential supply chain issues. Addressing the manufacturing maturity at this phase is a key in achieving program objectives in EMD.

2.2.10. Business Strategy

2.2.10.1. Small Business Innovation Research (SBIR) Technologies

2.2.10. Business Strategy

The Technology Development Strategy (TDS) should describe the contracts proposed to support the program's Technology Development Phase. Multiple competitive procurements may be required to investigate alternative technology approaches, mature critical technologies, and, acquire competitive prototypes and system design efforts, including the Preliminary Design

Review. Special attention should be given to the availability of documentation, such as a draft Capability Development Document, required to support the Request for Proposals for a contracted effort that includes preliminary system design.

Appropriate market research should be conducted prior to technology development to reduce the duplication of existing technology and products. The TDS should summarize the market research that has already been conducted, and the additional market research that is planned to be conducted prior the TD phase. Market research should yield an understanding of potential material solutions, their technology maturity, and potential sources, and should suggest strategies for acquiring them.

The TDS should address all elements of Business Strategy described in section 2.3.10, to include market research, contract types and incentives, strategies and application of competition throughout the program life cycle.

2.2.10.1. Small Business Innovation Research (SBIR) Technologies

Consistent with the direction of DoD Instruction 5000.02, the program manager (PM) should prepare a Technology Development Strategy (TDS) that appropriately uses the SBIR program to develop needed technologies, includes the use of technologies developed under the SBIR program, and gives fair consideration to successful SBIR technologies. During TDS preparation, the PM should ensure that the strategy addresses transition of relevant SBIR technologies and includes budgeting of follow-on funds for test, evaluation, and integration, as needed, to achieve the desired technological maturity. In addition, the PM should consider SBIR technologies as candidates for incremental and block system improvement initiatives as well as to address competitive prototyping requirements, particularly at the subsystems and component levels. To effectively leverage SBIR, the PM review and ensure compliance with DoD SBIR Phase III policy guidance and should engage their program office, Program Executive Office, systems command, product center, or DoD Component SBIR program coordinator for assistance. The PM should also consult the DoD SBIR program Web site for online resources and information including a program description, database of past awards and key points of contracts.

2.2.11. Resource Management

2.2.11.1. Program Office Staffing and Support Contractors – Organization

2.2.11.2. Cost and Funding

2.2.11.3. Cost Control

2.2.11.4. Earned Value Management (EVM)

2.2.11.5. Cost and Software Data Reporting

2.2.11. Resource Management

The Technology Development Strategy (TDS) should address program resource requirements and should consider changes in efforts as the program progresses. Personnel, cost control, advance procurement, the estimated program cost and potential perturbations in program funding should be taken into consideration in development of the TDS to increase the likelihood of successful program execution.

Strategies for cost reductions such as collaboration with other programs, greater reliance on commercial items, and competition should also be considered and described in the TDS.

2.2.11.1. Program Office Staffing and Support Contractors – Organization

The Technology Development Strategy (TDS) should address the planned personnel resources as derived via a time-phased workload assessment. The TDS should highlight:

- key manpower requirements
- functional competency requirements
- an extended staffing plan (e.g. legal expertise from command council or cost analysis support from a separate activity)

The TDS should include/ discuss:

- a program management office (PMO) organization chart that indicates what service fills the billet (for a joint program), whether it is filled with military, civilian or contractor personnel, what seniority level the billet is intended to be filled with, and whether the billet is currently filled, or vacant
- resource limitations that pose a risk to program/PMO success

2.2.11.2. Cost and Funding

The Technology Development Strategy (TDS) should address cost and funding status as well as track to budget information that includes appropriation (APPN), budget activity (BA), program element (PE), and the project, including the estimated logistic element costs to implement the sustainment strategy. This information is consistent with the track to budget information required in Selected Acquisition Reports (SARs). These charts give a strategic level overview of how the funding appropriated to the program is being spent and where in the budget the funds are coming from. Cost estimates for beyond the FYDP should be assigned a confidence level, and the anticipated appropriation types should be reflected as well.

The program manager (PM) should identify resource limitations that prevent the PM from pursuing a beneficial TDS or contracting approach. When such conditions exist, the PM should provide an estimate of any additional resources needed to implement the desired approach. A discussion should be included in the TDS describing how resources are planned to meet stated

objectives, including to what degree the program is funded relative to phase objectives and anticipated program requirements.

A funding chart like figure 2.2.11.2.F1 should be included as part of the TDS.

SAMPLE Investment Program Funding & Quantities											
($ in Millions / Then Year)	**Prior**	**FY09**	**FY10**	**FY11**	**FY12**	**FY13**	**FY14**	**FY15**	**FY10-15**	**To Comp**	**Prog Total**
RDT&E											
Prior $ (APPROVED BUDGET POSITION)	106.4	6.7	17.2	7.1	0.0	0.0	0.0	5.0	29.3	0.0	142.4
Current $ (PROPOSED BUDGET POSITION)	106.4	5.0	1.2	6.9	16.9	7.1	3.0	2.0	37.1	0.0	148.5
Delta $ (Current - Prior)	0.0	(1.7)	(16.0)	(0.2)	16.9	7.1	3.0	(3.0)	7.8	0.0	6.1
Required $	110.0	7.0	17.0	7.0	0.0	5.0	10.0	10.0	49.0	0.0	166.0
Delta $ (Current - Required)	(3.6)	(2.0)	(15.8)	(0.1)	16.9	2.1	(7.0)	(8.0)	(11.9)	0.0	(17.5)
PROCUREMENT											
Prior $ (APPROVED BUDGET POSITION)	0.0	128.3	145.2	133.5	0.0	0.0	1.0	2.3	282.0	1707.8	2,118.1
Current $ PROPOSED BUDGET POSITION)	0.0	89.6	104.6	90.0	94.0	93.7	87.0	84.2	553.5	1606.7	2,249.8
Delta $ (Current - Prior)	0.0	(38.7)	(40.6)	(43.5)	94.0	93.7	86.0	81.9	271.5	(101.1)	131.7
Required $	0.0	130.0	144.0	133.0	0.0	0.0	27.0	18.6	322.6	1700.0	2,152.6
Delta $ (Current - Required)	0.0	(40.4)	(39.4)	(43.0)	94.0	93.7	60.0	65.6	230.9	(93.3)	97.2
O&M											
Prior $ (APPROVED BUDGET POSITION)	53.3	3.5	14.5	2.3	1.6	0.0	2.0	2.8	23.2	0.0	80.0
Current $ (PROPOSED BUDGET POSITION)	71.4	4.2	0.9	4.3	14.2	5.2	5.0	4.6	34.2	0.0	109.8
Delta $ (Current - Prior)	18.1	0.7	(13.6)	2.0	12.6	5.2	3.0	1.8	11.0	0.0	29.8
Required $	78.3	12.0	7.0	3.0	2.5	0.0	5.0	3.4	20.9	0.0	111.2
Delta $ (Current - Required)	(6.9)	(7.8)	(6.1)	1.3	11.7	5.2	0.0	1.2	13.3	0.0	(1.4)
TOTAL											

Prior $ (APPROVED BUDGET POSITION)	159.7	138.5	176.9	142.9	1.6	0.0	5.0	10.1	336.5	0.0	634.7
Current $ (PROPOSED BUDGET POSITION)	177.8	98.8	106.7	101.2	125.1	106.0	91.0	90.8	620.8	0.0	897.4
Delta $ (Current - Prior)	18.1	(39.7)	(70.2)	(41.7)	123.5	106.0	86.0	80.7	284.3	0.0	262.7
Required $	188.3	149.0	168.0	143.0	2.5	5.0	32.0	32.0	382.5	0.0	719.8
Delta $ (Current - Required)	(10.5)	(50.2)	(61.3)	(41.8)	122.6	101.0	59.0	58.8	238.3	0.0	177.6
QUANTITIES											
Prior (APPROVED BUDGET POSITION)	0	552	681	587	0	0	3	124	1395	0	1,947
Current (PROPOSED BUDGET POSITION)	0	445	467	376	382	379	355	358	2317	0	2,762
Delta Qty (Current - Prior)	0	(107)	(214)	(211)	382	379	352	234	922	0	815
Required Qty	0	440	450	376	382	379	332	332	2251	0	2,691
Delta Qty (Current - Required)	0	5	17	0	0	0	23	26	66	0	71

Figure 2.2.11.2.F1. Sample Investment Program Funding and Quantities

NOTE: Chart for the TDS Phase should include phase Funding, and Quantities that are more in line with prototypes – consistent with technology development phase expectations – NOT Engineering and Manufacturing Development and Production.

Click here for a funding chart with instructions.

A track to budget chart, including all appropriations, like the ones in a SAR should accompany the funding chart. An example could look like this:

Track To Budget - Perfectly Funded Acquisition Program (PFAP)

RDT&E

APPN 1319 BA 05 PE 0604269N (Navy) Project 3063 PFAP Development

Procurement

APPN 1506 BA 01 PE 0204154N (Navy) ICN 0143 APN-1 PFAP Platform

APPN 1506 BA 06 PE 0204154N (Navy) ICN 0605 APN-6 PFAP Spares

MILCON
APPN 1205 PE 0204154N (Navy)

2.2.11.3. Cost Control

The Technology Development Strategy (TDS) should document plans to control program costs. Cost control tools and processes should be summarized.

2.2.11.4. Earned Value Management (EVM)

The Technology Development Strategy (TDS) should make clear a program's intent to comply with EVM requirements.

EVM is a key integrating process in the management and oversight of acquisition programs. It is a management approach that combines both government management requirements and industry best practices to ensure the total integration of cost, schedule, and work scope aspects of contracts.

Pre-MDAP and pre-MAIS efforts should implement the DoD EVM requirements on applicable contracts, subcontracts, and other agreements as prescribed in DoD Instruction 5000.02, this Defense Acquisition Guidebook, and the EVM Implementation Guide (EVMIG). EVM Systems (EVMS) that comply with the guidelines in American National Standards Institute/Electronic Industries Alliance Standard 748 (ANSI/EIA-748) should be used to plan and control the performance of applicable contracts. A Contract Performance Report (CPR) and an Integrated Master Schedule (IMS) should be required for applicable contracts. In addition, Integrated Baseline Reviews (IBRs) should be conducted for applicable contracts. The applicable Defense Federal Acquisition Regulation Supplement (DFARS) clauses should be used to place the EVM requirements in solicitations and contracts.

2.2.11.5. Cost and Software Data Reporting

The two components of the Cost and Software Data Reporting (CSDR) system are the Contractor Cost Data Reporting (CCDR) and Software Resources Data Reporting (SRDR). PMs shall use the CSDR system to report data on contractor costs and resource usage incurred in performing DoD programs.

A summary of the OSD CAIG-approved CSDR plans – both for the overall program and for each contract – for the TD Phase shall be addressed in the TDS for ACAT I programs. If the OSD CAIG Chairman has waived this requirement, then a summary of the grounds for waiving the requirement should be discussed in the "Tailoring" section of the TDS.

2.2.12. Program Security Considerations

The Technology Development Strategy (TDS) program security summary should describe the processes planned to protect the overall effort/program from threats, including adversaries, industrial espionage and threats to personal information, and including unfair competition. The TDS should address design and programmatic measures/counter-measures to protect the program's technologies and capabilities. Cyber and IT security should be considered across the life cycle. The TDS should identify the technical, schedule, cost, and funding issues associated with protecting critical program information and technologies, and the plans to resolve the issues.

The TDS should contain a list of known or probable critical program information (CPI) and potential countermeasures such as anti-tamper in the preferred system concept and in the critical technologies and competitive prototypes.

Concurrent with managing technology integration risk during TD and identifying the preliminary critical technology elements, programs should integrate a process to select Critical Program Information (CPI) during this phase. Doing so enables PMs to also consider the risk of foreign targeting and collection of key or critical technologies that if compromised to an adversary could result in the system being rendered ineffective on the battlefield, significantly affect the longevity of the system, and/or enables an adversary to significantly enhance their military capability and threaten US battlefield superiority.

A recommended process to identify CPI is available in DoD 5200.1M, and Chapter 8 of this guidance provides additional detail.

Upon identification of CPI, a Program Protection Plan (PPP) is implemented as required by DoDI 5200.39. If a PPP has already been developed it should be summarized in the TDS briefly and sufficiently to ensure the MDA that appropriate measures are planned and funded, or that more resources are needed (e.g. include whether anti-tamper measures are planned).

The PPP is a single-source reference document that provides all the information needed to ensure CPI is appropriately protected, the assurance necessary to the MDA that the program has taken appropriate measures, and/or inform the MDA that more protection may be required which could require more funding needed to ensure CPI is protected. The PPP is designed to ensure the program meets its objectives by ensuring CPI, which is essential to system assurance, is not compromised.

In addition to formal requirements to protect classified information there is a need to protect controlled unclassified information (CUI), and personally identifiable information (PII) in a changing threat environment. Provisions should be made in the Acquisition Strategy for any contracts that generate or use CUI, or PII to provide for protection of that information and flow down such requirements to subcontractors and vendors as appropriate. It is recommended that programs include adequate protection of CUI and PII as threshold requirements for source selection.

For additional guidance see section 2.3.12.

2.2.13. Test Planning

The Technology Development Strategy (TDS) contents regarding test planning should include major events or planned accomplishments, summary context for technical maturation plans, and discussions of how test planning may impact the overall cost, schedule or performance of the phase. More comprehensive test planning details for the TD Phase are the subject of the Test and Evaluation Strategy (TES). The TES provides a test plan describing how technology demonstration(s) will be evaluated to determine whether the goals and exit criteria for the TD Phase are achieved. The TES provides more comprehensive information for test and evaluation during the TD Phase.

2.2.14. Data Management Strategy and Technical Data Rights

All new technology development and system design efforts should be assessed for long-term technical data needs and reflect the assessment in a Data Management Strategy (DMS). The DMS should reflect the assessment and integration of the data requirements across all the functional disciplines required to develop, manufacture and sustain the system over the life cycle. Restricted use and intellectual property rights should be minimized. The DMS must be approved in the context of the Technology Development Strategy prior to issuing a contract solicitation.

The PM should consult 10 USC 2320, DoD Instruction 5000.02, Enclosure 12, paragraph 9, and DFARS to determine appropriate DMS content.

If the TDS will also serve as the Acquisition Plan, consideration for DFARS 207.106 and 227.7100 needs to be observed and addressed in the DMS section of the AS.

The DMS should be integrated with other life-cycle sustainment planning, and consider all forms of recorded information, regardless of the method of recording, and include both government and contractor-created data.

The DMS should include:

- an assessment of the data required to design, and an initial assessment of the data required to manufacture and sustain the system. Further consideration of the data requirements should include support for competition or re-competition for development, production, sustainment, or upgrades; and
- an assessment of, including a priced contract option for, the future delivery of technical data and intellectual property rights not acquired upon initial contract award and shall consider the contractor's responsibility to verify any assertion of restricted use and release of data.

2.2.15. Life-Cycle Sustainment Planning

The initial supportability strategy and related sustainment metrics should be included in the Technology Development Strategy (TDS). The approach for achieving the required enabling sustainment technologies to implement the support strategy and achieve the sustainment metrics should be discussed in the TDS. Any risks to achieving the necessary support structure for the time frame of the program by IOC should be identified and a mitigation strategy outlined. The specific enabling support technologies should be identified along with the corresponding plan to technically mature each support element.

Systems entering acquisition at MS-B or C should include sustainment planning in their Acquisition Strategy. TDS sustainment planning data will support LCSP development.

2.2.16. Life-Cycle Signature Support Plan (LSSP)

An LSSP is required for validated and approved signature dependent programs (see DoDD 5250.01) and the LSSP should be included in the Technology Development Strategy (TDS). A signature dependent program is a defense acquisition that uses or is comprised of a sensor, system, or process that relies on signatures or signature data to successfully perform a task or mission. The LSSP should be developed during the Materiel Solution Analysis and TD Phases.

The TDS should describe signature support requirements and required funding to support program-related efforts. The requirements and required funding should be developed in concert with the Intelligence Community and the Senior Signature Management Forum.

If the LSSP needs to be classified to fulfill the information requirement it should be so noted in the unclassified TDS and a classified LSSP annex of the TDS should be handled separately. Such a classified annex may combine with the CPI/PPP summary as described in Section 2.2.12.

Applicable acquisition programs need to identify, capture, and address the signatures essential to the development, testing, fielding, operation, and maintenance of required weapons, smart munitions, sensors, and systems capabilities at each program milestone and prior to proceeding to the Low-Rate Initial Production (LRIP), production and/or fielding decision.

During EMD and/or P&D the LSSP should be matured.

2.2.17. Chemical, Biological, Radiological, and Nuclear (CBRN) Survivability

The Technology Development Strategy (TDS) should discuss the activities planned to address the CBRN mission-critical system's CBRN survivability requirements and assess its CBRN survivability during the TD Phase.

In accordance with DoD Instruction 3150.09, all CBRN mission-critical systems under development, regardless of Acquisition Category, are required to address CBRN survivability at each milestone. A mission-critical system is one whose operational effectiveness and operational suitability are essential to successful mission completion or to aggregate residual combat capability. If this system fails, the mission likely will not be completed. Such a system can be an auxiliary or supporting system, as well as a primary mission system. CBRN mission critical is that subset of mission-critical systems with operational concepts requiring employment and survivability in a CBR environment or a nuclear environment. CBRN survivability is the capability of a system to avoid, withstand, or operate during and/or after exposure to a CBR environment (and relevant decontamination) or a nuclear environment, without losing the ability to accomplish the assigned mission. CBRN survivability is divided into CBR survivability, which is concerned with CBR contamination including fallout, and nuclear survivability, which covers initial nuclear weapon effects, including blast, EMP and other initial radiation and shockwave effects.

2.3. Systems Acquisition: Acquisition Strategy

The Acquisition Strategy is a comprehensive, integrated plan that identifies the acquisition approach, and describes the business, technical, and support strategies that management will follow to manage program risks and meet program objectives. The Acquisition Strategy should define the relationship between the acquisition phases and work efforts, and key program events such as decision points, reviews, contract awards, test activities, production lot/delivery quantities, and operational deployment objectives. The Acquisition Strategy also defines the approach to provide maximum practicable opportunities to small business, including small disadvantaged business, women-owned small business, veteran-owned small business, service-disabled small business and Historically Underutilized Business Zones.

The Acquisition Strategy guides program execution across the entire program life cycle, focusing primarily on the upcoming phase. The strategy evolves over the phases and should continuously reflect the current status and desired end point of the phase and the overall program. An MDA-approved update to the Acquisition Strategy is required prior to Milestone C and FRP (or Full Deployment Decision).

DoD Instruction 5000.02 requires an approved Acquisition Strategy prior to Milestone B approval and prior to any final RFP release for the EMD phase or later. The Acquisition Strategy should be updated for all subsequent major decisions and program reviews, and whenever the approved strategy changes. The Acquisition Strategy is approved by the MDA.

The Acquisition Strategy establishes the milestone decision points and acquisition phases planned for the program. The strategy should cover development, testing, production, and life-cycle support. It should establish the requirements for each phase, and identify the critical management events. The Acquisition Strategy should include a Top Level Integrated Schedule and a summary of highlights from the Integrated Master Plan and Integrated Master Schedule.

The Acquisition Strategy is a key document to support the statutory Milestone B certification (seeDAG Chapter 10). The Milestone B (program initiation for ships) Acquisition Strategy should describe plans to complete the EMD phase and meet the Production decision entry criteria including: acceptable performance in developmental test and evaluation and operational assessment (OSD OT&E oversight programs); mature software capability; no significant manufacturing risks; manufacturing processes under control (if Milestone C is full-rate production); an approved Capability Production Document (CPD); a refined integrated architecture; acceptable interoperability; acceptable operational supportability; and demonstration that the system is affordable throughout the life cycle, fully funded, and properly phased for rapid acquisition.

Additionally the Milestone B Acquisition Strategy should reflect plans to attain a stable design in the EMD Phase (including detail design for ships), prior to the start of production (prior to start of construction for ships). In support of those plans, some criteria for design stability include: successfully completing event-driven successful technical reviews; achieving a mature product model/design configuration (with defined design stability parameters, maturity levels to be achieved and inclusion of key design artifacts such as vendor assurance information); consistency between the User's CONOPS and the validated operational requirements/capabilities. Also, for shipbuilding the Acquisition Strategy should reflect plans regarding allowance for design process flexibility to effectively manage obsolescence and ship construction and delivery schedule requirements.

For entry into production the Milestone C Acquisition Strategy should be based on having satisfied all the criteria in the previous two paragraphs. The Milestone C Acquisition Strategy should reflect planned efforts to result in completion of manufacturing development in order to ensure adequate and efficient manufacturing capability and to produce the minimum quantity necessary to provide production or production-representative articles for IOT&E, establish an initial production base for the system; and permit an orderly increase in the production rate for the system, sufficient to lead to full-rate production upon successful completion of operational (and live-fire, where applicable) testing. Additionally the MS C Acquisition Strategy should reflect plans for demonstrating control of the manufacturing process and acceptable reliability, the collection of statistical process control data, and the demonstrating control and capability of other critical processes such as successful IOT&E.

For entry into Full-Rate Production (FRP) the Acquisition Strategy should be based on having satisfied all the criteria in the previous paragraph. The FRP Acquisition Strategy should reflect planned efforts to deliver the fully funded quantity of systems, supporting materiel, and services for the program or increment to allow the users attain Initial Operational Capability (IOC).

2.3.1. Acquisition Approach

2.3.1. Acquisition Approach

The Acquisition Strategy defines the approach the program will use to achieve full capability: either evolutionary or single step; it should include the rationale to justify the choice including appropriate reference to the capability document. The DoD preference is evolutionary acquisition. When a program uses an evolutionary Acquisition Strategy, each increment and/or sub-program should have a specific set of parameters with thresholds and objectives appropriate to the increment.

In an evolutionary approach, the Acquisition Strategy should fully describe the initial increment of capability (i.e., the initial deployment capability), and how it will be funded, developed, tested, produced, and supported. The Acquisition Strategy should preview similar planning for subsequent increments, and identify the approach to integrate and/or retrofit earlier increments with later increment improvements. Program strategies for subsequent increments should be contained in separate documents, or be included as annexes to the core program strategy document.

If the capability documents do not allocate increments of capability (leading to full capability) to specific program increments consistent with an evolutionary approach, the PM should work closely with the user/sponsor to determine whether an evolutionary acquisition approach will serve the user/sponsor needs. Where necessary and acceptable to the user/sponsor, the acquisition community should work with the requirements community to modify the capability documents.

The approved Acquisition Strategy should address the proposed management approach to be used to define both the capability and the strategy applicable to each increment. This discussion should specifically address whether end items delivered under early increments will be retrofitted with later increment improvements. Additionally, if increments will deliver varying materiel solutions for different applications this should be discussed in the Acquisition Strategy as well.

The information included in the Acquisition Strategy should be complete enough to fully describe the planning considerations and decisions needed to balance cost, schedule and life-cycle performance. The strategy to track and measure progress against the KPPs and any cost or schedule driving KSAs should be briefly described. Highlighting the flexibility, or challenges, for using the trade space between KPPs is also appropriate. The Acquisition Strategy also addresses resources and business strategy such as small business utilization at the prime and subcontracting level. Because the Acquisition Strategy establishes the breadth of a program's efforts including such essential aspects of a program as the degree of competition, contract type, and incentive arrangements, the Acquisition Strategy must be approved by the MDA per DoD Instruction 5000.02 before a final RFP is released, a synopsis is published, a Justification and Approval is approved, or negotiations undertaken.

If the PM decides to incorporate concurrency in the program, the Acquisition Strategy should discuss the benefits and risks of the concurrency and address the resultant risk mitigation and

testing impacts. The Department's preferred approach is for event driven, rather than schedule driven, acquisition strategies.

For programs approaching LRIP, i.e., a Milestone C Acquisition Strategy, if planned LRIP quantities are proposed to exceed 10 percent of the total quantity a rationale should be provided in the ‘Tailoring' section of the Acquisition Strategy.

If a lead system integrator is planned to be employed, the Acquisition Strategy should include a discussion of checks and balances to maintain government responsibility for acquisition activities and inherently governmental functions. Additionally, it should be clearly illustrated that the contract is not awarded to a contractor that either has or is expected to acquire a direct financial interest in the development or construction of an individual system or an element of a system of systems.

2.3.1.1. Modular Open Systems Approach (MOSA) Summary

The program manager (PM) should plan for a modular open systems approach (MOSA) implementation and include a summary of such planning as part of the overall Acquisition Strategy.

MOSA is the DoD implementation of "open systems." The PM should incorporate MOSA principles into the Acquisition Strategy to ensure access to the latest technologies and products, and to facilitate affordable and supportable system development and modernization of fielded assets.

The summary of open system planning should describe how MOSA fits into a program's overall acquisition process. A more detailed description of open system planning may be appropriate in the Systems Engineering Plan (SEP), IAW the SEP Preparation Guide. If upon completing a business case analysis, the PM decides to acquire a system with closed interfaces, the PM should report to the MDA, in context of the Acquisition Strategy, the justification for the decision. The justification should describe the potential impacts on the ability to access latest technologies from competitive sources of supply throughout the system life cycle, integrate the system with other systems in a joint integrated architecture venue, and to integrate and/or retrofit earlier increments with later increments in an evolutionary acquisition context.

2.3.1.2. Tailoring

Consistent with statutory and federal regulatory requirements, the program manager (PM) and Milestone Decision Authority (MDA) may tailor the phases and decision points for a program to meet the specific needs of the program. Tailoring should consider program category, risk, urgency of need, and technology maturity. Tailoring of regulatory information requirements and processes must be approved by the MDA prior to, or in accordance with, the strategy being approved, or execution in such a fashion. Tailoring of statutory information requirements and processes can only be done in rare cases and may require justification to Congress.

Note that 10 USC 2366b requires the MDA to certify, prior to Milestone B approval that the program complies with all relevant policies, regulations, and directives of the Department of Defense.

The tailoring section of the Acquisition Strategy should contain proposed tailoring initiatives for MDA approval, as well as already approved (e.g., via ADM) tailoring plans., and be complemented by rationale for why the policies, regulations or directives being proposed to be tailored are not relevant. If no tailoring of Department policy is being proposed it should be so stated.

For shipbuilding programs, the section should describe the timing for obtaining MDA authorization for start of production, the timing for the milestone C decision point, the definition of LRIP quantity, the Full Rate Production Decision Review, and any intermediate DAE level reviews to authorize ship procurements or other key events in the shipbuilding program beyond Milestone B or program initiation. Also discuss the plan for any tailoring in the timing of regulatory document submissions to support these reviews.

For example: In a Milestone B or C Acquisition Strategy, if the proposed LRIP quantities exceed 10 percent of the total production quantity, the rationale for the higher quantities should be provided in the tailoring section of the Acquisition Strategy.

2.3.2. Source and Related Documents

The Acquisition Strategy should cite key source documents, such as and as a minimum, include:

- the underpinning approved capability documents(s) (e.g. CDD)
- the most recent AoA
- the TEMP
- the SEP
- the Information Support Plan
- the Acquisition Information Assurance Strategy
- the PPP (for programs with CPI)
- the Programmatic ESOH Evaluation (PESHE) with National Environmental Policy Act (NEPA)/EO 12114 Compliance Schedule
- any relevant or recent ADM

Each citation should include the approval date and note the approval status. If a document is still in draft and not approved, it should be so noted and the projected approval date provided.

Some of the cited documents (e.g., PPP) need to be summarized elsewhere in the Acquisition Strategy, in addition to being cited as a source document.

2.3.3. Capability Needs

To provide context, the Acquisition Strategy should contain a summary description of the capability the acquisition is intended to satisfy or provide. The summary should highlight system characteristics driven by interoperability and/or joint integrated architectures, capability areas, and family or system of systems.

This summary description should have significant commonality with the "Mission & Description" section of the Selected Acquisition Report (SAR)

A listing of the unclassified Key Performance Parameters (KPPs) and cost, schedule or performance driving KSAs from the reference capability document should be included in the Acquisition Strategy. Only if the entire Acquisition Strategy is classified due to significant other information sections should classified KPPs or KSAs be included in the Acquisition Strategy. An unclassified Acquisition Strategy should refer to the appropriate source document (e.g., CDD, or APB) for a listing of the classified KPPs and/or KSAs.

The Life-cycle Signature Support Plan (LSSP) TDS content requirements are described in DAG section 2.3.16 and should ideally be included in the Capability Needs section of the TDS.

2.3.4. Top-Level Integrated Schedule

2.3.4.1. Engineering and Manufacturing Development (EMD) Top-Level Integrated Schedule

2.3.4.2. Milestone C and Full Rate Production Top-Level Schedule

2.3.4. Top-Level Integrated Schedule

A top-level integrated master schedule should be included in the Acquisition Strategy that focuses on the current phase, but also projects the entire life cycle of the program. Two schedule figures may be used as it is useful to have one for the current phase, and a second one for the entire life cycle.

The schedule should be reflective of event-based planning. If the planning is schedule-driven then an explanation and rationale should be provided. Event-driven is the preferred schedule planning method for the Department.

The schedule should tie together the major events of the program including: major milestones, procurement events, technical reviews, testing events and prototype or product deliveries.

2.3.4.1. Engineering and Manufacturing Development (EMD) Top-Level Integrated Schedule

When preparing an Acquisition Strategy for EMD the document should focus primarily on the EMD phase, but include the life cycle to disposal and a short summary of past events.

The EMD Acquisition Strategy must be approved by the MDA prior to final EMD Request for Proposals (RFP) release per DoD Instruction 5000.02 and should show the approval date for the CDD, and the completion dates for prior systems engineering Technical Reviews (e.g. SRR, SFR, and PDR) were completed. EMD activities that should be identified include:

- contract events such as contract definitization, planned exercising of contract line item numbers, Integrated Baseline Review (IBR), and future contract events in preparation for the Production and Deployment (P&D) phase such as the RFP for which an Acquisition Strategy update should be approved
- systems engineering technical reviews appropriate in the EMD phase include the Critical Design Review (mandated at the system level) and followed by the mandated Post-CDR Report and MDA-chaired Assessment, the Test Readiness Review, Physical Configuration Audit, System Verification Review, and Production Readiness Review.
- major sustainment related efforts to be accomplished in contract(s) and government organizations with focus on the EMD phase. The schedule should include key sustainment planning activities as well as materiel and data development and deliveries including but not limited to the following
    - Maintenance Plans (initial and "final")
    - depot maintenance core capabilities stand-up
    - Training Plan
    - Source of Repair Assignment Process (SORAP)
    - ESOH plans and considerations

Other key acquisition events and information such as technology demonstrations, prototypes, plans to demonstrate product support capabilities and/or long lead contract activities should be included. Additionally, the schedule should include a summary of projected Milestone C information including CPD initiation and approval, development of the Production and Deployment phase Acquisition Strategy; the Test and Evaluation Master Plan, and Systems Engineering Plan, etc.

2.3.4.2. Milestone C and Full Rate Production Top-Level Schedule

When preparing the initial Acquisition Strategy for the Production and Deployment (P&D) Phase the document should emphasize the P&D/Low-Rate Initial Production (LRIP) phase (for MDAPs and major systems) or limited deployment (for automated information system), address the life cycle to disposal, and limit detail on past events. If/when the Acquisition Strategy is updated for the FRP decision the emphasis should be on production and sustainment efforts and their impact on cost, schedule and performance.

When submitting an Acquisition Strategy for Milestone C, the document should include a schedule that shows approval/completion dates for the CPD and the Initial Production Baseline (IPB) were completed, the EMD contract awarded, and the preceding technical reviews completed.

The schedule should show when the program plans to have a Milestone C review to enter into the P&D Phase as well as tentative plans for events to meet the requirements of FRP or Full Deployment (FD) if automated information system, including activities/events planned through the Operations and Support Phase to Disposal.

Tentative plans should identify LRIP Systems, IOC, FOC, plans for a product support package/PBL implementation, technical reviews, a RFP that will result in a LRIP contract, an IBR, a RFP that will result in a Production Contract, and an IBR that will become the Final Production Baseline.

Technical reviews needed for FRP or FD include an Assessment of Operational Test Readiness (AOTR) and Operational Test Readiness Review (OTRR) prior to Initial Operational Test and Evaluation (IOT&E), review of Live Fire Test and Evaluation (LFT&E), and Interoperability/ Sustainment Reviews. Once the program enters FRP the program should begin Follow-On Operational Test and Evaluation (FOT&E). Post-IOC sustainment reviews will be supported by the LCSP.

Major sustainment related efforts to be accomplished via contract(s) and government effort for the P&D phase should be discussed. The schedule should include key sustainment planning activities including but not limited to the following:

- Sustainment contract awards
- Maintenance Plans
- depot maintenance core capabilities stand-up
- Training Plan
- Source of Repair Assignment Process (SORAP)
- Identify the activation schedule for each site in the supply chain required to support the system including the maintenance sites (including depots) and training sites. Indicate the schedule for any required hardware or software (including support and test equipment, trainers, etc.) needed at each site.

2.3.5. Program Interdependency and Interoperability Summary

If the program is dependent on the outcome of other acquisition programs or must provide capabilities to other programs, those relationships should be detailed in the acquisition strategy.

The Acquisition Strategy should describe the treatment of interoperability requirements. For example, if an evolutionary Acquisition Strategy involves successive increments satisfying time-phased capability needs, the PM should address each increment and the transitions from increment to increment. The Acquisition Strategy should identify any waivers or deviations that have been requested, obtained, or expected to be requested. The Strategy should reflect full compliance with the interoperability considerations discussed in section 4.4.10 and for Information Technology, including National Security Systems, sections 7.3 and 7.6.

Information Interoperability. The PM should identify and assess the impact of technical, schedule, cost, and funding critical path issues related to information interoperability that could impact the PM's ability to execute the Acquisition Strategy. The PM should also identify critical path issues in related program(s) or system(s) that will exchange information with the PM's delivered system) and assess their potential impact.

Other-than Information Interoperability. The PM should identify and assess the impact of technical, schedule, cost, and funding critical path issues related to general interoperability concerns for the PM's acquisition program. The PM should also identify any critical path issues in other program(s) or system(s) that will interoperate with or otherwise materially interact with the PM's delivered system and assess the potential impact of the systems (e.g., fuel formulation and delivery systems, mechanical connectors, armament, or power characteristics).

Coalition Interoperability. The growing requirement for effective international coalitions requires a heightened degree of international interoperability. Reciprocal trade, international standardization agreements, and international cooperative programs with allies and friendly nations serve that end. The acquisition community should strive to deploy and sustain systems, equipment, and consumables that are inherently interoperable with our potential coalition partners.

2.3.6. International Cooperation

2.3.6.1. Testing Requirements for Export of Defense Systems

2.3.6. International Cooperation (See Also Section 11.2)

The PM should include a discussion of the international cooperative strategy sufficient to satisfy the statutory (10 USC 2350a) requirement for a Cooperative Opportunities document. In addition, E1.1.13 of the DoD Directive 5000.01 requires coalition interoperability from DoD systems, units and forces.

To streamline the required documentation for acquisition programs, AT&L has developed a template for a coalition interoperability section of Acquisition Strategies that includes the cooperative opportunities document requirement for 10 USC 2350a.

Considerations required are:

- a statement indicating whether or not a project similar to the one under consideration by the DoD is in development or production by any NATO country, Major Non-NATO Ally, or friendly foreign country.
- if a project similar to the one under consideration by the DoD is in development or production by any NATO country, Major Non-NATO Ally, or friendly foreign country, an assessment is to be provided by the PM for the USD(AT&L) as to whether that project

could satisfy, or could be modified in scope so as to satisfy, the military requirements of the project of the United States under consideration by the DoD
- an assessment of the advantages and disadvantages with regard to program timing, developmental and life-cycle costs, technology sharing, and Rationalization, Standardization, and Interoperability (RSI) of seeking to structure a cooperative development program any NATO country, Major Non-NATO Ally, or friendly foreign country.
- the recommendation as to whether the DoD should explore the feasibility and desirability of a cooperative development program with one or more countries and any NATO country, Major Non-NATO Ally, or friendly foreign country.

The International Cooperation section of the Acquisition Strategy should address the PM's plan to meet the warfighter's requirements and to increase the opportunity for coalition interoperability as part of the developing DoD program.

Alternatives examined should include:

- existing defense programs and materiel from foreign sources that meet US requirements or can be modified to meet US requirements
- existing NATO or commercial standards that promote interoperable systems
- considerations for future use of system with coalition partners in operations
- opportunities for reciprocal defense trade and cooperation
- new cooperative research, development, test and evaluation projects with allied and partner nations to reduce U.S. costs and risk, and improve coalition capabilities of U.S. and partner systems
- shared production and logistics support in order to strengthen alliances and partnerships with NATO allies, non-NATO allies, and strategic partners
- interface and security requirements to support foreign military sales, or direct commercial sales of U.S. system

PMs have a responsibility to look across the breadth of the program to understand the numerous opportunities to engage the international community to the benefit of the United States, consistent with information security and technology transfer limitations.

To assist with the assessment, PMs should coordinate with their respective international programs offices to gain insight into international activities which may impact their program. This process should continue throughout the life cycle of the program and begin to reap tangible outcomes as the program progresses towards completion.

The requirements are discussed in depth further in the Coalition Interoperability Template.

2.3.6.1. Testing Requirements for Export of Defense Systems

An ACAT I or II system that has not successfully completed Developmental Test and Evaluation (DT&E) and IOT&E requires USD(AT&L) approval prior to any foreign military sale, commitment to sell, or DoD agreement to license for export. This does not preclude Government-sponsored discussions of potential cooperative opportunities with allies, or reasonable advance business planning or marketing discussions with potential foreign customers by defense contractors, provided appropriate authorizing licenses are in place.

2.3.7. Risk and Risk Management

The PM should establish a risk management process consistent with sections 4.2.3.1.5 and 4.4.7.5, and summarize the process in the Acquisition Strategy.

The PM should summarize the anticipated or existing key acquisition risks for the program and include the related risk cube. The risk cube format should be taken from the Risk Management Guide for DoD Acquisition, 6th Edition, Version 1, August 2006. The Acquisition Strategy should describe how funding, schedule and performance are planned to be balanced and traded to manage/mitigate key risks.

If the program is so complex and technically challenging that it would not be practicable to reduce program risk to a level that would permit the use of a fixed-price type contract, the AS should include an explanation of the level of program risk. The explanation also needs to include steps that have been taken, and are planned, to reduce risk. Finally, the rationale for granting a Milestone B approval for entry into EMD, despite the high level of program risk, should be included in this explanation. This explanation of complexity, technical challenge, risk, and rationale, will provide the MDA with the needed documentation if other than a fixed-price type contract is to be used for EMD.

The EMD phase AS should define how the program will ensure its design is sufficiently mature before Milestone C (entry point into production). Design stability should be established through completion of basic and functional design and 3D product modeling (when employed). The AS should define the level of maturity of the design product model and other key design artifacts, including vendor information, needed to ensure that the design is stable.

ESOH Risks are assessed in accordance with MIL-STD-882D and are summarized in the ESOH section of the Acquisition Strategy. Only those ESOH risks that have been also been identified as program risks should be included in this section.

Spectrum risk may result in significant program risk. Spectrum analysis must be done for all applicable programs. For more information see DAG Chapter 7.6.

The Acquisition Strategy is an appropriate place to discuss cost, schedule and performance implications or trades related to risks and risk mitigation, but not for detailed mitigation plans with waterfalls etc. The SEP is the document appropriate for details on mitigation plans for the noted key technology-related acquisition risks. The SEP or the program's Risk Management Plan

is appropriate for detailed discussion of the risk management process, whereas the Acquisition Strategy should only contain a summary.

2.3.8. Technology Maturation

The TDS is subsumed into the Acquisition Strategy in preparation for Milestone B and the EMD phase, and most of the TDS information contents are distributed throughout the Acquisition Strategy. This is apparent from the similarities of sections 2.2 and 2.3. This Technology Maturation section of the Acquisition Strategy should focus on the strategy to mature technology, in concert with integration and design development efforts, to reach the desired level at the next Milestone. For instance, an EMD Acquisition Strategy being approved prior to Milestone B approval should describe the strategy to mature critical technology elements from TRL 6 to at least meet a goal of TRL 7 prior to the planned Critical Design Review, or meet the TRL 7 requirement by Milestone C. Because technology maturity needs to be evaluated in a ‘relevant environment' for TRL 6, and an ‘operational environment' for TRL 7, the "environment definition" specific to the subject program also belongs in this section of the Acquisition Strategy. Additional detqails can be found in The TRA Deskbook.

Software maturity strategy should be discussed in this section of the Acquisition Strategy.

Key sustainment enabling technology to meet the program's KPPs and KSAs should also be discussed in this section of the Acquisition Strategy.

Prototyping and CP for technology maturation and end item integration to meet the needs described in section 2.3.3, Capability Needs, should be described in the Acquisition Strategy.

Major events such as proof testing and the overall schedule and resources for the upcoming Milestone Technology Readiness Assessment should be discussed in this section of the Acquisition Strategy.

2.3.9. Industrial Capability and Manufacturing Readiness

2.3.9. Industrial Capability and Manufacturing Readiness

The development of the Acquisition Strategy should include results of industrial base capability (public and private) analysis to design, develop, produce, support, and, if appropriate, restart an acquisition program. This includes assessing manufacturing readiness and effective integration of industrial capability considerations into the acquisition process and acquisition programs ensuring the sufficient maturity before production begins. For applicable products, the Acquisition Strategy should also address the approach to making production rate and quantity changes in response to contingency needs. Consider these items in developing the strategy:

- Technology and Industrial Base, including small business
- Design
- Cost and Funding
- Materials
- Process Capability and Control
- Quality Management
- Manufacturing Personnel
- Facilities
- Manufacturing Management

2.3.9.1. Industrial Capability

The program office should assess the impact of programmatic decisions on the national and international technology and industrial base supporting U.S. defense to satisfy the requirements of 10 USC 2440 and DFAR Subpart 207.1. Overall Industrial Capabilities Assessments (ICAs) should address critical sub-tier, as well as prime contractor capabilities and should include:

- new and unique capabilities that must be developed or used to meet program needs
    - identify DoD investments needed to create new or enhance existing industrial capabilities. This includes any new capability (e.g. skills, facilities, equipment, etc).
    - identify new manufacturing processes or tooling required for new technology. Funding profiles must provide for up front development of manufacturing processes/tooling and verification that new components can be produced at production rates and target unit costs.
    - identify exceptions to FAR Part 45, which requires contractors to provide all property (equipment, etc) necessary to perform the contract.
- program context in overall prime system and major subsystem level industry sector and market
- strategies to address any suppliers considered to be vulnerable
- risks of industry being unable to provide new program performance capabilities at planned cost and schedule
- alterations in program requirements or acquisition procedures that would allow increased use of non-developmental or commercial capabilities
- strategies to deal with product or component obsolescence, given DoD planned acquisition schedule and product life

- strategies to address reliability issues (i.e., tampering, potential interrupted delivery from non-trusted sources, etc.) associated with commercial components for sensitive applications
- strategies to utilize small business, including small disadvantaged business, women-owned small business, veteran-owned small business, service-disabled veteran-owned small business and small businesses located in Historically Underutilized Business Zones.

2.3.9.2. Elevating Industrial Capability Issues

While not specific to the Acquisition Strategy, program offices and the Military Services are encouraged to resolve identified industrial capability issues at the lowest level possible. However, there are cases when issues may impact more than a single program or Service. A program office should elevate an industrial capabilities matter via their Program Executive Officer to the Office of the Deputy Under Secretary of Defense (Industrial Policy) when an item produced by a single or sole source supplier meets one or more of the following criteria (even if the program office has ensured that its program requirements can and/or will be met):

- it is used by three or more programs
- it represents an obsolete, enabling, or emerging technology
- it requires 12 months or more to manufacture
- it has limited surge production capability

2.3.9.3. Industrial and Manufacturing Readiness

For Major Defense Acquisition Programs and major systems with production components, the Acquisition Strategy should highlight the strategy for assessing industrial and manufacturing readiness. During the Engineering and Manufacturing Development (EMD) and Production and Deployment (P&D)/Low-Rate Initial Production (LRIP) Phases, the industrial and manufacturing readiness should be assessed to identify remaining risks prior to a full-rate production go-ahead decision.

The EMD Acquisition Strategy should define how the program management office will assess that the industrial capabilities are capable to support program requirements through the P&D and Operations and Support (O&S) phases. The P&D Acquisition Strategy for approval at Milestone C should update the assessment process, including relevant findings thus far, and highlight any risks that may have been identified.

The EMD Acquisition Strategy should also highlight the strategy for assessing the manufacturing processes to ensure they have been effectively demonstrated in an appropriate environment, such as a pilot line environment, prior to Milestone C. The manufacturing environment should incorporate key elements (equipment, personnel skill levels, materials, components, work instructions, tooling, etc.) required to produce production configuration items, subsystems or systems that meet design requirements in low rate production. To the maximum extent practical,

the environment should utilize rate production processes using production processes forecasted to be used in LRIP. The Acquisition Strategy should strategically describe the EMD phase planning to assess and demonstrate that the manufacturing processes/capabilities, required for production will have been matured to a level of high confidence for building production configuration products in the P&D phase.

For Milestone C, key manufacturing readiness considerations include:

- industrial base viability
- design stability
- process maturity
- supply chain management
- quality management
- facilities
- manufacturing skills availability

Sources of data to inform industrial and manufacturing readiness could include; technical reviews and audits, Program Status Reviews, pre-award surveys, Production Readiness Reviews, Industrial Capabilities Assessments, trade-off studies, tooling plans, make-or-buy plans, manufacturing plans, and bills of material. An important output includes actions to reduce or address any remaining risks.

The Milestone C Acquisition Strategy should provide the status of the assessments of the manufacturing processes highlight needed steps to progress from an EMD manufacturing environment to an LRIP environment.

For the Full Rate Production Decision Review Acquisition Strategy update, the Program should identify remaining risks prior to a production go-ahead decision. Key considerations should include industrial base viability, design stability, process maturity, supply chain management, quality management, and facilities and manufacturing skills availability. Sources of data could include technical reviews and audits, Program Status Reviews, pre-award surveys, Production Readiness Reviews, Industrial Capabilities Assessments, trade-off studies, tooling plans, make-or-buy plans, manufacturing plans, and bills of material. Important outputs include actions to reduce or handle remaining risks.

If a program/Service is already utilizing Manufacturing Readiness Levels (MRLs), and wishes to use them in the Acquisition Strategy discussion of manufacturing readiness, the MRL definitions in use would need to be supplied as well.

2.3.9.4. Sustaining Industrial Capabilities

In many cases, commercial demand now sustains the national and international technology and industrial base. The following considerations will improve public and private capabilities to respond to DoD needs:

- Defense acquisition programs should minimize the need for new defense-unique industrial capabilities
- Foreign sources and international cooperative development should be used where advantageous and within limitations of the law (DFARS Part 225)
- The Acquisition Strategy should promote sufficient program stability to encourage industry to invest, plan, and bear their share of the risk. However, the strategy should not compel the contractor to use independent research and development contracts, except in unusual situations where there is a reasonable expectation of a potential commercial application
- Prior to completing or terminating production, the DoD Components should ensure an adequate industrial capability and capacity to meet post-production operational needs
- Where feasible, Acquisition Strategies should consider industrial surge requirements and capability for operationally-expendable items such as munitions, spares, and troop support items. These are likely surge candidates and should receive close attention and specific planning, to include use of contract options. The program office should identify production bottlenecks at both the prime and sub-tier supplier levels for high use/high volume programs in an asymmetric warfare construct. Surge capability can be included in evaluation criteria for contract award
- When there is an indication that industrial capabilities needed by DoD are endangered, an additional analysis is required as the basis for determining what – if any – DoD action is required to preserve an industrial capability (see DoDD 5000.60 and DoD 5000.60-H). Considerations for the analysis include:
    - DoD investments needed to create or enhance certain industrial capabilities
    - The risk of industry being unable to provide program design or manufacturing capabilities at planned cost and schedule
    - If the analysis indicates an issue beyond the scope of the program, the PM should notify the MDA and PEO
    - When the analysis indicates that industrial capabilities needed by the DoD are in danger of being lost, the DoD Components should determine whether government action is required to preserve the industrial capability
    - The analysis should also address product technology obsolescence, replacement of limited-life items, regeneration options for unique manufacturing processes, and conversion to performance specifications at the subsystems, component, and spares levels.

DoDD 5000.60 imposes oversight restrictions on any proposed action or investment to preserve an industrial capability for an acquisition program. Any such investment with an anticipated cost of equal to or less than $10 million annually must be approved by the appropriate milestone decision authority, and any investment with a cost greater than $10 million annually must be approved by the USD (AT&L).

2.3.10. Business Strategy

A description of the planned strategy to contract for the major program efforts, including services and end items, should be summarized in the Acquisition Strategy. This should include the extent to which the strategy is focused in traditional transactions based processes and performance based/outcome processes. Specific contracts (in place and/or planned) and contracting plans should be addressed in the Business Strategy portion of the Acquisition Strategy. Initial planning and consideration for the use of small business and small business innovation research should also be addressed here.

Market research, competition and incentive strategies should be discussed in the business strategy section of an Acquisition Strategy. Market research needs to be done to identify capable sources of supply to promote competitive best value acquisitions, to evaluate the possibilities for commercial and/or non-developmental materiel solutions, to assess all size business capabilities and the status of the marketplace. Competition should be employed to drive pricing and affordability wherever possible, and a well planned incentive strategy should support the accomplishment of cost and/or schedule goals.

A program manager should host a procurement planning forum(s) with appropriate elements of the program and/or PEO staff to establish the value items and services that shall be used by the finance, logistics/user, and procurement communities. The forum would include representation from all of the functional elements of the communities, each one representing their respective equity in the process. The perspective of the vendor also needs to be known and considered based on Program Office experience with Requests for Information (RFIs), pre-proposal conferences and draft Requests for Proposals (RFPs). DFARS 204.71 should be followed. The Program Manager and Contracting Officer need to lead the efforts to align requirements throughout the ‘require' to ‘inventory' process. These discussions then form the basis for a business requirement in addition to a mission requirement so that critical enterprise priorities like internal controls, financial statement, asset valuation, and material accountability are postured in the resultant contract(s), rather than extrapolated after the fact. The forum members should agree on the level of detail appropriate for uniform reporting throughout all phases of the procurement cycle which include: requirement identification (procurement request), contracting, accounting, performance (including shipment and receiving), acceptance, payment, property management, inventory accountability, and reordering functions. Since to the extent that these events are severable, separate line items should be used and all line items must be made available as data throughout all steps of the process. The program manager needs to ensure program budget requirements are in place to accommodate the level of effort required to establish this detail in business systems starting with requirement generation.

RFIs are initial indicators to industry regarding acquisition goals and possible objectives, as well as serving the government with needed information. The RFP process initiates a potential government-industry relationship that needs to be bound by mutual understanding of expectations to ensure the greatest chances for success. RFIs and RFPs need to be thoughtfully planned with respect to the type and amount of information that is included. Translation of government expectations to industry is done best with a comprehensive RFP. For these reasons, the Technology Development Strategy (TDS) or Acquisition Strategy and technical planning

documents such as the Systems Engineering Plan and the Test & Evaluation Master Plan should be appropriately developed for, and heavily referenced in, the RFP process. Virtually any/all information elements in a TDS or Acquisition Strategy relate to processes and efforts that may drive cost, schedule and/or performance in a given acquisition program or pre-program. Final RFPs for a given phase, or any succeeding acquisition phase, can not be released, nor any action be taken that would commit the pre-program or program to a particular contracting strategy, until the MDA has approved the respective Acquisition Strategy for that phase (TDS for the Technology Development Phase; Acquisition Strategy for succeeding phases).

2.3.10.1. Small Business and Small Business Innovation Research

2.3.10.1.1. Subcontracting Plan / Small Business Participation

2.3.10.1.2. Performance Measurement

2.3.10.1.3. Small Business Innovation Research (SBIR) Consideration

2.3.10.1. Small Business and Small Business Innovation Research

It is the policy of the United States that small business, veteran-owned small business, service-disabled veteran-owned small business, Historically Underutilized Business Zone small business, small disadvantaged business, and women-owned small business concerns shall have the maximum practicable opportunity to participate in performance of contracts and subcontracts (15 USC 631-657(f)). The acquisition strategy should consider small business utilization in accordance with guidance provided in FAR Part 19 and DFARS Part 219, Small Business Programs. In addition, FAR Part 15.3 and DFARS Part 215.3, Source Selection, require that past performance information be used in source selection evaluations. The PM should consult the local small business specialist or the Office of Small Business Programs.

2.3.10.1.1. Subcontracting Plan / Small Business Participation

When FAR 19.7 applies, the acquisition strategy must include a requirement for submission of a subcontracting plan. The strategy should establish maximum practicable individual socio-economic subcontracting goals, meaningful small business work, incentives which have small business participation. In addition, the acquisition strategy should outline planned award evaluation criteria concerning small business utilization in accordance with FAR 15.3, and DFARS Subpart 215.3 regarding source selection. Additionally, program Acquisition Strategies should document the rationale for the selection of the planned subcontract tier or tiers, and that prime contractors give full and fair consideration to qualified sources other than the prime contractor for the development and/or production of major subsystems and components of major weapon systems.

2.3.10.1.2. Performance Measurement

The acquisition strategy should outline the program manager's plan for measuring the achievement of socio-economic goals and evaluating performance as it relates to small business utilization. The Contractor Performance Assessment Reporting System (CPARS) is an automated system for contractor performance information that is used throughout the DoD.

2.3.10.1.3. Small Business Innovation Research (SBIR) Consideration

Consistent with the direction of DoD Instruction 5000.02, the PM should include SBIR and give fair consideration to successful SBIR-funded technologies in Acquisition Strategy planning. Note that SBIR follow-on development and acquisition (Phase III, not funded with the SBIR set-aside budget) may be able to be pursued on a sole-source basis without further competition. Competition for Phase I and Phase II awards (contracts funded by the SBIR set-aside budget) satisfies all statutory competition requirements. SBIR Phase III contract awards have SBIR status and thus must be accorded SBIR data rights. SBIR Phase III work may be pursued directly through Phase III contracts or encouraged through subcontracts via incentives. To effectively leverage SBIR, the PM review and ensure compliance with DoD SBIR Phase III policy guidance and should engage their program office, Program Executive Office (PEO), systems command, product center, or Component SBIR program coordinator for assistance.

2.3.10.2. Contract Approach

2.3.10.2.10. Incorporation of Systems Engineering Requirements

2.3.10.2. Contract Approach

The events set forth in contracts should support the exit criteria for the phase.

2.3.10.2.1. Performance-Based Business Strategy

Consistent with a Performance-Based Business Environment as described in FAR Part 37.6, Performance-Based Acquisition, the Acquisition Strategy should include a performance-based business strategy throughout the life cycle.

2.3.10.2.2. Modular Contracting

The PM should use modular contracting, as described in FAR Section 39.103, for major IT acquisitions, to the extent practicable. Similarly, before an agency can consolidate contract requirements with an estimated value exceeding $5.5M, DFARS 207.170-3 requires the Acquisition Strategy must contain the results of market research, alternative contracting approaches, and a determination by the senior procurement executive that the consolidation is necessary and justified.

2.3.10.2.3. Contracting Bundling or Consolidation

FAR 7.103(s) requires that acquisition planners, to the maximum extent practicable, avoid unnecessary and unjustified bundling that precludes small business participation as contractors. As a result of this direction, DoD Instruction 5000.02 requires a Benefit Analysis and Determination. The purpose of the benefit analysis is to determine the relative benefit to the government among two or more alternative procurement strategies. (See definitions at FAR 2.201 and DFARS 207.170-2)

DFARS 207.170 directs agencies not to consolidate contract requirements with an estimated total value exceeding $5.5million unless the acquisition strategy includes: (1) the results of market research: (2) Identification of any alternative contracting approaches that would involve a lesser degree of consolidation; and (3) a determination by the senior procurement executive that the consolidation is necessary and justified.

The PM should consult the local small business representative or Office of Small Business Programs website for additional information concerning this information requirement or any acquisition planning.

2.3.10.2.4. Major Contract(s) Planned

For each major contract (greater than $40 million (then year dollars) for an MDAP and greater than $17 million for MAIS), planned to execute the Acquisition Strategy, the Acquisition Strategy should describe what the basic contract buys; how major deliverable items are defined; options, if any, and prerequisites for exercising them; and the events established in the contract to support appropriate exit criteria for the phase or intermediate development activity.

2.3.10.2.4.1. Contract Type Selection

Per Section 818 NDAA FY 2007, for MS B approval, the MDA shall select a contract type that is consistent with the level of program risk. The MDA may select from a fixed-price, including fixed price incentive, or cost type contracts.

NDAA 2007, Section 818 states that the "MDA may authorize the use of a cost type contract" upon determination that:

1. the program is complex and technically challenging that it would not be practicable to reduce program risk to a level that would permit the use of a fixed-price contract
2. the complexity and technical challenge of the program is not the result of a failure to meet the requirements established in section 2366a of title 10, United States Code.

The text of these two preceding bullets must be included verbatim in the AS to meet the intent of Section 818, and for MS B approval, and combined with supporting documentation, if a cost type contract is to be used.

The MDA may authorize the use of a cost type contract if the determination is made that the program is complex and technologically challenging; therefore not reducing program risk level for the use of a fixed-price contract and the complexity and technical challenge of the program is not the result of a failure to meet the requirements in 10 USC 2366b. The MDA shall document the contract type selected, to include an explanation of the program risk level and the steps, if necessary, to reduce high program risk in order to proceed to MS B. If this documentation is placed in the Risk and Risk Management section (see 2.3.10.5) of the AS rather than in the Contract Type Selection section of the AS, the Contract Type Selection section will reference the Risk and Rick Management section.

2.3.10.2.4.2. Sustainment Procurement Strategy

The AS should provide an overview of the sustainment related contract(s) including how the integrated product support package will be acquired. The discussion should include the:

- Type contract and length along with major terms and conditions
- Performance measures being used (including the extent to which it is traditional transaction based/process focused and performance-based/outcome focused)
- Sustainment related functions, hardware or data covered in each contract
- Portion of system covered by performance based product support strategy

2.3.10.2.5. Multi-Year Contracting

In accordance with 10 USC 2306b, the Acquisition Strategy should address the PM's consideration of multiyear contracting for full rate production, and address the PM's assessment of whether the production program is suited to the use of multiyear contracting based on the requirements in FAR Subpart 17.1. Similarly, the Acquisition Strategy should address the PM's consideration of the criteria of 10 USC 2306c when considering a multiyear contract for "covered" services.

If the acquisition strategy calls for a multi-year service contract (as distinguished from contracts that span multiple years–see FAR Subpart 17.1 and DFARS Subpart 217.171 the strategy shall address compliance with 10 USC 2306c and OMB Circular A-11. OMB Circular A-11 requires that multiyear service contracts be scored as operating leases. Therefore, the Acquisition Strategy shall address the budget scorekeeping that will result from use of the proposed contracting strategy.

2.3.10.2.6. Contract Incentives

In the Contract Incentives section, the Acquisition Strategy should explain the planned contract incentive structure and how the PM plans to employ contract incentives to achieve required cost, schedule, and performance outcomes. If more than one incentive is planned for a contract, the Acquisition Strategy should explain how the incentives complement each other and do not interfere with one another.

2.3.10.2.7. Warranties

The PM should examine the value of warranties on major systems and pursue them when appropriate and cost-effective. If appropriate, the PM should incorporate warranty requirements into major systems contracts in accordance with FAR Subpart 46.7. Warranty program data should be included in the Life-cycle Sustainment Plan.

2.3.10.2.8. Leasing

The PM should consider the use of leasing in the acquisition of commercial vehicles and equipment whenever the PM determines that leasing of such vehicles is practicable and efficient. Leases are limited to an annual contract with no more than a 5-month lease option.

The PM may not enter into any lease with a term of 18 months or more, or extend or renew any lease for a term of 18 months or more, for any vessel, aircraft, or vehicle, unless the PM has considered all costs of such a lease (including estimated termination liability) and has determined, in writing, that the lease is in the best interest of the Government (10 USC 2401a and DFARS 207.4). It should be noted that a lease of more than 12 months does not permit the extension of one year funding authority.

Leases of equipment to meet a valid need under the provisions of CJCS Instruction 3170.01 will be categorized in accordance with the criteria in DoD Instruction 5000.02.

For further guidance on leasing, see Office of Management and Budget (OMB) Circular A-11, Appendix B, Budgetary Treatment of Lease-Purchases and Leases of Capital Assets; and OMB Circular A-94, Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs.

Additionally 10 USC 2401 must be met for long-term services contracts where the contractor will use a vessel, aircraft or combat vehicle to perform the services. This statute (Section 2401) also applies to long-term leases and charters of vessels, aircraft and combat vehicles. This statute bars entry into such a contract unless the Secretary of a military department has been specifically authorized by law to enter the contract. Section 2401 requires the Secretary of the military department must notify Congressional committees before issuing a solicitation for such a contract. Section 2401 also requires the Secretary must notify the committees of detailed information regarding the proposed contract and must certify that certain criteria and laws have been satisfied (as set out in Section2401).

2.3.10.2.9 Developmental Testing Requirements

Developmental testing requirements should be appropriately addressed in the translation of operational requirements into contract specifications, in the source selection process, and in the preparation of requests for proposals.

2.3.10.2.10 Incorporation of Systems Engineering Requirements

The Acquisition Strategy should ensure systems engineering requirements, including reliability, availability, maintainability, and lifecycle management and sustainability requirements, are incorporated into contract requirements for each major defense acquisition program.

2.3.10.3. Market Research

FAR Part 10 requires the Acquisition Strategy include the results of completed market research and plans for future market research. (See also the JCIDS Manual). Market research information provided in the Acquisition Strategy should be sufficient to satisfy the requirements of 10 USC 2366b. For the Milestone B certification, compliance with 10 USC 2377, 15 USC 644, WSARA Sec 202, other statute & DFARs determines the outcome of the market strategy certification element. Market research should yield an understanding of potential material solutions, their technology maturity, and potential sources, and should suggest strategies for acquiring them.

Market research is a primary means of determining the availability and suitability of commercial items and the extent to which the interfaces for these items have broad market acceptance, standards-organization support, and stability. In addition, market research is important in seeking

small business capabilities. Thorough market research needs to be performed to determine whether or not small businesses are capable of satisfying the requirements. Market research supports the acquisition planning and decision process, supplying technical and business information about commercial technology and industrial capabilities to arrive at the most suitable approach to acquiring, distributing and supporting supplies and services. Market research, tailored to program needs should continue throughout the acquisition process and during post-production support.

2.3.10.4. Competition

Competition is a key consideration for fostering innovation and affordability for defense applications. The Acquisition Strategy for all programs should describe the competition planned for all phases of the program's life cycle, or explain why competition is not practicable or not in the best interests of the Government. To promote synergies that facilitate competition and innovation, the PM should, where feasible, identify other applications for the technologies in development within the functional capability areas identified by the Joint Staff.

Acquisition Strategies for Major Defense Acquisition Programs shall describe the measures taken to ensure competition or the option of competition, at both the prime and subcontract level throughout the program life-cycle. The measures may include the following: Competitive prototyping, dual-sourcing, unbundling of contracts, funding of next-generation prototypes or subsystems, use of modular, open architectures to enable competition upgrades (See DAG section 2.3.1.1), use of build-to-print approaches to enable production through multiples sources, acquisition of complete technical data packages (See DAG section 2.3.14.1 and periodic competition for sub-system upgrades, licensing of additional suppliers. Additionally, program Acquisition Strategies shall document the rationale for the selection of the planned subcontract tier or tiers, and that prime contractors to give full and fair consideration to qualified sources other than the prime contractor for the development or construction of major subsystems and components of major weapon systems(See DAG section 2.3.10.1.1).

2.3.11. Resource Management

2.3.11. Resource Management

The Acquisition Strategy should address program resource requirements and should consider changes in efforts as the program progresses. Personnel, cost control, advance procurement, the estimated program cost and potential perturbations in program funding should be taken into consideration in development of the Acquisition Strategy to increase the likelihood of successful program execution.

Strategies for cost reductions such as collaboration with other programs, greater reliance on commercial items, and competition should also be considered and described in the Acquisition Strategy.

2.3.11.1. Program Office Staffing and Support Contractors – Organization

The Acquisition Strategy should address the planned personnel resources as derived via a time-phased workload assessment. The Acquisition Strategy should highlight:

- key manpower requirements
- functional competency requirements
- an extended staffing plan (e.g. legal expertise from command council or cost analysis support from a separate activity)

The Acquisition Strategy should include/discuss:

- program management office (PMO) organization chart that indicates what service fills the billet (for a joint program), whether it is filled with military, civilian or contractor personnel, what seniority level the billet is intended to be filled with, and whether the billet is currently filled, or vacant.
- Resource limitations that pose a risk to program/PMO success.

2.3.11.2. Cost and Funding

The Acquisition Strategy should address cost and funding status as well as track to budget information that includes appropriation (APPN), budget activity (BA), program element (PE), and the project name. This information is consistent with the track to budget information required in Selected Acquisition Reports (SARs). These charts give a strategic level overview of how the funding appropriated to the program is being spent and where in the budget the funds are coming from.

The logistics (O&M) portion of the cost breakdown structure in the funding chart should include the cost estimates and funding available to implement the sustainment concept to meet the schedule laid out in the integrated schedule. It should include the funding required for each of the logistics elements required to implement the LCSP including any sustainment contracts, new or upgraded facilities, support equipment, trainers, etc.- Sustainment Development and Acquisition Costs: Include the Logistics Requirements and Funding Summary (LRFS). It should provide a detailed breakout of the sustainment related funding required and budgeted by

year and appropriation for the main sustainment cost categories consistent with the Acquisition Program Baseline and Cost Analysis Requirements Description (CARD). - Ownership/Operating & Support Costs: Using constant year dollars, provide the O&S Cost estimates including the "operating unit" annual costs and total costs over an extended period. The supporting drivers (e.g. number of years and inventory levels) and major assumptions consistent with the Sustainment Quad chart should be provided.

The PM should identify resource limitations that prevent the PM from pursuing a beneficial Acquisition Strategy or contracting approach. If required, the PM should provide an estimate of any additional resources needed to implement the desirable strategy or approach. A discussion should be included in the Acquisition Strategy describing how resources are planned to meet program baseline parameters, including to what degree the program is funded relative to thresholds or objectives.

A funding chart like figure 2.3.11.2.F1 should be included as part of the Acquisition Strategy.

SAMPLE Investment Program Funding & Quantities											
($ in Millions / Then Year)	**Prior**	**FY09**	**FY10**	**FY11**	**FY12**	**FY13**	**FY14**	**FY15**	**FY10-15**	**To Comp**	**Prog Total**
RDT&E											
Prior $ (APPROVED BUDGET POSITION)	106.4	6.7	17.2	7.1	0.0	0.0	0.0	5.0	29.3	0.0	142.4
Current $ (PROPOSED BUDGET POSITION)	106.4	5.0	1.2	6.9	16.9	7.1	3.0	2.0	37.1	0.0	148.5
Delta $ (Current - Prior)	0.0	(1.7)	(16.0)	(0.2)	16.9	7.1	3.0	(3.0)	7.8	0.0	6.1
Required $	110.0	7.0	17.0	7.0	0.0	5.0	10.0	10.0	49.0	0.0	166.0
Delta $ (Current - Required)	(3.6)	(2.0)	(15.8)	(0.1)	16.9	2.1	(7.0)	(8.0)	(11.9)	0.0	(17.5)
PROCUREMENT											
Prior $ (APPROVED BUDGET POSITION)	0.0	128.3	145.2	133.5	0.0	0.0	1.0	2.3	282.0	1707.8	2,118.1
Current $ PROPOSED BUDGET POSITION)	0.0	89.6	104.6	90.0	94.0	93.7	87.0	84.2	553.5	1606.7	2,249.8
Delta $ (Current -	0.0	(38.7)	(40.6)	(43.5)	94.0	93.7	86.0	81.9	271.5	(101.1)	131.7

Prior)											
Required $	0.0	130.0	144.0	133.0	0.0	0.0	27.0	18.6	322.6	1700.0	2,152.6
Delta $ (Current - Required)	0.0	(40.4)	(39.4)	(43.0)	94.0	93.7	60.0	65.6	230.9	(93.3)	97.2
O&M											
Prior $ (APPROVED BUDGET POSITION)	53.3	3.5	14.5	2.3	1.6	0.0	2.0	2.8	23.2	0.0	80.0
Current $ (PROPOSED BUDGET POSITION)	71.4	4.2	0.9	4.3	14.2	5.2	5.0	4.6	34.2	0.0	109.8
Delta $ (Current - Prior)	18.1	0.7	(13.6)	2.0	12.6	5.2	3.0	1.8	11.0	0.0	29.8
Required $	78.3	12.0	7.0	3.0	2.5	0.0	5.0	3.4	20.9	0.0	111.2
Delta $ (Current - Required)	(6.9)	(7.8)	(6.1)	1.3	11.7	5.2	0.0	1.2	13.3	0.0	(1.4)
TOTAL											
Prior $ (APPROVED BUDGET POSITION)	159.7	138.5	176.9	142.9	1.6	0.0	5.0	10.1	336.5	0.0	634.7
Current $ (PROPOSED BUDGET POSITION)	177.8	98.8	106.7	101.2	125.1	106.0	91.0	90.8	620.8	0.0	897.4
Delta $ (Current - Prior)	18.1	(39.7)	(70.2)	(41.7)	123.5	106.0	86.0	80.7	284.3	0.0	262.7
Required $	188.3	149.0	168.0	143.0	2.5	5.0	32.0	32.0	382.5	0.0	719.8
Delta $ (Current - Required)	(10.5)	(50.2)	(61.3)	(41.8)	122.6	101.0	59.0	58.8	238.3	0.0	177.6
QUANTITIES											
Prior (APPROVED BUDGET POSITION)	0	552	681	587	0	0	3	124	1395	0	1,947
Current (PROPOSED BUDGET POSITION)	0	445	467	376	382	379	355	358	2317	0	2,762
Delta Qty	0	(107)	(214)	(211)	382	379	352	234	922	0	815

(Current - Prior)											
Required Qty	0	440	450	376	382	379	332	332	2251	0	2,691
Delta Qty (Current - Required)	0	5	17	0	0	0	23	26	66	0	71

Figure 2.3.11.2.F1. Sample Investment Program Funding and Quantities

Click here for a funding chart with instructions. The funding chart that is approved as part of the AS is subject to change as the ICE and APB evolve.

A track to budget chart, including all appropriations, like the ones in a Selected Acquisition Report should accompany the funding chart. An example could look like this:

Track To Budget - Perfectly Funded Acquisition Program (PFAP)

RDT&E

APPN 1319 BA 05 PE 0604269N (Navy) Project 3063 PFAP Development

Procurement

APPN 1506 BA 01 PE 0204154N (Navy) ICN 0143 APN-1 PFAP Platform

APPN 1506 BA 06 PE 0204154N (Navy) ICN 0605 APN-6 PFAP Spares

MILCON

APPN 1205 PE 0204154N (Navy)

2.3.11.3. Cost Control and Cost as an Independent Variable (CAIV) Plan

The Acquisition Strategy should document plans to control program costs, specifically Program Acquisition Unit Cost, Average Procurement Unit Cost, and Life-Cycle Cost. Cost control tools and processes should be summarized.

If a CAIV approach is planned it should be described. Included should be strategies for teaming between the program management office, financial estimating and management communities, the war fighter/user and requirements community to define cost goals and trade space; ensuring capability base processes, and how the cost-performance trade process is to be executed. If a CAIV approach is not planned the overall cost control approach should be justified and the rationale for not using CAIV principles explained.

The two components of the Cost and Software Data Reporting (CSDR) system are the Contractor Cost Data Reporting and Software Resources Data Reporting. PMs shall use the CSDR system to report data on contractor costs and resource usage incurred in performing DoD programs.

A summary of the OSD Cost Analysis Improvement Group (CAIG)-approved CSDR plans – both for the overall program and for each contract – for the Engineering and Manufacturing Development and P&D phase shall be addressed in the Acquisition Strategy for ACAT I programs. If the OSD CAIG Chairman has waived this requirement, then a summary of the grounds for waiving the requirement should be discussed in the "Tailoring" section of the Acquisition Strategy.

2.3.11.4. Earned Value Management (EVM)

EVM is a key integrating process in the management and oversight of acquisition programs. It is a management approach that combines both government management requirements and industry best practices to ensure the total integration of cost, schedule, and work scope aspects of contracts.

Compliance with DoD EVM requirements are the same as those for the TDS, spelled out in section 2.2.11.4.

The Acquisition Strategy should make clear a program's intent to comply with EVM requirements.

2.3.11.5. Advance Procurement

If advance procurement of long lead items is planned it should be so stated in the strategy.

DoD Financial Management Regulation 7000.14-R requires that the procurement of end items be fully funded, i.e., the cost of the end items to be bought in any fiscal year should be completely included in that year's budget request. However, there are times when it is appropriate to procure some components, parts, materiel, or effort in advance of the end item buy. These items are referred to as advance procurements. Statutory authority for these advance procurements should be provided in the relevant authorization and appropriations acts.

Advance procurement funds are used in major acquisition programs for advance procurement of components whose long-lead times require purchase early in order to reduce the overall

procurement lead-time of the major end item. Advance procurement of long lead components is an exception to the DoD "full funding" policy and must be part of the President's budget request. These expenditures are subject to the following limitations:

- the cost of components, material, parts, and effort budgeted for advance procurement should be low compared to the total cost of the end item
- the PM judges the benefits of the advance procurement to outweigh the inherent loss of or limitation to future MDA flexibility
- the MDA approves the advance procurement
- the procurement received statutory authority, as discussed above

As part of the milestone review, the MDA should approve specific exit criteria for advance procurement. These specific exit criteria should be satisfied before the PM releases any advance procurement funding for either the initial long lead-time items contract(s) or the contract(s) for individual, follow-on, long lead-time lots. The contracts office should initiate a separate contract action for advance procurement of long lead materiel.

The MDA must approve advance procurement in advance of Milestone C, and the intention should be clearly noted in the Acquisition Strategy. A template should be completed and provided for MDA approval prior to executing long lead advance procurement. The template can be included in the AS, or by separate memo for the MDA to approve.

2.3.12. Program Security Considerations

2.3.12. Program Security Considerations

The Acquisition Strategy program security summary should describe the processes planned to protect the overall effort/program from threats, including adversaries, industrial espionage and threats to personal information, and including unfair competition. The Acquisition Strategy should address design and programmatic measures/counter-measures to protect the program's technologies and capabilities. Cyber and IT security should be considered across the life cycle. The Acquisition Strategy should also describe the processes planned to be used to identify critical program information (CPI) and, if applicable, measures for the protection of CPI, including protction of critical functionality from supply chain risk in accordance with DODI 5200.39 adn DTM 08-048, "Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems". The Acquisition Strategy should identify the technical,

schedule, cost, and funding issues associated with protecting critical program information and technologies, and the plans to resolve the issues.

In addition to formal requirements to protect classified information there is a need to protect controlled unclassified information (CUI), and personally identifiable information (PII) in a changing threat environment. Provisions should be made in the Acquisition Strategy for any contracts that generate or use CUI, or PII to provide for protection of that information and flow down such requirements to subcontractors and vendors as appropriate. It is recommended that programs include adequate protection of CUI and PII as threshold requirements for source selection.

2.3.12.1. Information Assurance

In this section, 2.3.12.1, the term "Acquisition Strategy" refers both to the Acquisition Strategy and the TDS.

The PM should ensure that the Acquisition Strategy identifies the significant technical, schedule, cost, and funding issues associated with implementing Information Assurance into the system being acquired. The purpose of the IA section in a program's Acquisition Strategy is to clearly convey to the reader all IA issues that will impact the acquisition of material or services in support of the system acquisition. It is the means of highlighting to the acquisition team those IA considerations that must be included in solicitations or contracts, or purchased, arranged through supporting memoranda of understanding/agreement, secured through Service Level Agreements, or acquired from another agency via a MIPR. In short, it should identify anything IA-related that substantively impacts the program's acquisition activities.

IA requirements should addressed throughout the system life cycle in accordance with DoD Directive 8500.01E, DoD Instruction 8500.2, and DoD Instruction 8510.01 (DIACAP)

The Acquisition Strategy should address any significant IA technical considerations that may impact the acquistion, such as requirements for IA products or IA-enabled products, or cryptographic devices. Prior to system integration, these items must be evaluated by NSA, NIST or other qualified laboratories depending on their characteristics, and will require careful planning to avoid negatively impacting the program's schedule.

The Acquisition Strategy should summarize significant IA related test events, and/or such events on the critical path or with strong interplay on other schedule sequencing. More detailed IA related test events should be addressed in the TEMP.

IA related cost drivers or significant investments should be highlighted in the Acquisition Strategy. IA specific costs include Information Systems Security Engineering (ISSE) support, development/procurement, test & evaluation, and certification & accreditation of the IA architecture. It also includes operations and maintenance costs related to maintaining the system security posture following deployment.

If the program is resource constrained (e.g. funding or personnel) for IA execution it should be addressed briefly in the IA section of the Acquisition Strategy, and more thoroughly in the Resources section (see section 2.3.11)

Section 7.5.9.5 provides a template containing examples of IA considerations that may be tailored for inclusion in the Acquisition Strategy. When it is required, the planning for and documentation of the program's Acquisition IA Strategy should produce the information required for this section (see section 7.5.5).

2.3.12.2. Critical Program Information and Program Protection Plan Summary

This section is applicable for programs with critical program information and lists the information that should be provided in the Acquisition Strategy. If the critical program information process found no critical program information, the date of the assessment and the approving authority should be cited. Additionally, a written statement that no PPP is necessary should be explicitly made, and a date for re-initiating the critical program information process identified.

A recommended process to identify CPI is available in DoD 5200.1-M, and Chapter 8 of this guidance provides additional detail.

When critical program information is found the PPP should be identified as one of the source documents in the Acquisition Strategy, and an unclassified summary of the critical program information should be included. If the appropriate information cannot be provided at an unclassified level a classified annex will need to be created and so noted in this section of the unclassified Acquisition Strategy. Such a classified annex may combine with the LSSP summary as described in Section 2.3.16.

A summary of threats and status of threat assessments should be provided. A risk assessment, focused on the likelihood of attack and severity of impact, should be presented in the Acquisition Strategy Countermeasures employed by the program should be described, to include:

- Information Assurance measures (e.g. IA control implementation; use of DoD Information Assurance Certification and Accreditation Process (DIACAP) or other verification process) applied to DoD information systems and to contractor systems containing program CPI
- Anti-Tamper
- Physical Security
- Supply Chain RIsk Management Key Practices employed
- Other applicable countermeasures identified in the PPP

Identify the cost and schedule impacts to the overall program due to program protection needs, including whether or not those impacts are within the scope of the program as planned and baselined.

2.3.12.3. Anti-Tamper Measures

The PM should ensure the Acquisition Strategy is consistent with the anti-tamper measures of section 8.5.3. The program manager should plan and budget for AT throughout the systems life cycle to include post-production validation of the AT implementation.

2.3.12.4. Supply Chain Risk Management (SCRM) Key Practices

Program protection planning processes should consider the exposure of critical functionality and/or technology to supply chain risk during the program lifecycle. The supply chain for critical components should be evaluated for supply chain threat by leveraging all source threat analyses developed by DIA Threat Assessment Center (TAC), and mitigated by means of SCRM Key Practices.

2.3.13. Test and Evaluation (T&E)

Consistent with the direction of DoD Instruction 5000.02, the PM should integrate developmental and operational testing throughout the acquisition process. The Acquisition Strategy should describe the knowledge and products needed from T&E, and their timing, to inform acquisition decisions and milestones across the life cycle. Test plans with significant and direct influence on program cost, schedule, or performance should be addressed in the Acquisition Strategy. Sections of the Test and Evaluation Master Plan (TEMP) can be referenced in the Acquisition Strategy if such detail is considered relevant to the Acquisition Strategy.

The PM should engage the Test and Evaluation Working-Level Integrated Product Team (T&E WIPT) in the development of the Acquisition Strategy, and harmonize the Acquisition Strategy and the test and evaluation strategy, e.g. the TEMP.

While test and evaluation discussion is necessary for a complete Acquisition Strategy, detailed information is not appropriate for the Acquisition Strategy. However, detailed test and evaluation planning information is located in the Test and Evaluation Strategy or TEMP, depending on the milestone.

2.3.14 Data Management

2.3.14.1. Data Management Strategy and Technical Data Rights

2.3.14.2. Integrated Data Environment

2.3.14.1 Data Management

The PM must prepare a Data Management Strategy (DMS) as part of the Acquisition Strategy for ACAT I and II programs. All program plans shoul be assessed for short and long-term technical data needs and that assessment reflected in the Data management Strategy (DMS). The DMS should reflect the assessment and integration of the data requirments across all the functional disciplines required to develop, manufacture and sustain the system over teh life cycle. The PM should review 10 USC 2320, Public Law 109-364, DoD Instruction 5000.02, Enclosure 12, paragraph 9, and DFARS 227 to determine the necessary content. Further requirements information can be found in section 4.2.3.1.7 and 5.1.6 of this document.

If the AS is also planned to serve as the Acquisition Plan, DFARS 207.106 adn 227.7100 should be considered and adderssed in the DMS section of the AS.

The DMS must be approved and integrated in the Acquisition Strategy and integrated with other life-cycle sustainment planning prior to issuing a contract solicitation. It should address all forms of recorded information, regardless of the method of recording, and include both government and contractor-created data. The DMS should include:

- an assessment of the data required to design, manufacture, and sustain the system, as well as to support re-competition for production, sustainment, or upgrades; and
- an assessment of, including a priced contract option for,the future delivery of technical data and intellectual property rights not acquired upon initial contract award
- and shall consider the contractor's responsibility to verify any assertion of restricted use and release of data
- consideration of teh government's rights to the data acquired including requirements for delivery and access in instances wehre the government does not possess unlimited rights.

2.3.14.2. Integrated Data Environment

The PM should summarize in the Acquisition Strategy plans to establish a cost-effective data management system and digital environment.

PMs should establish a data management system within the IDE that allows every activity involved with the program to cost-effectively create, store, access, manipulate, and exchange digital data. This includes, at minimum, the data management needs of the system engineering process, modeling and simulation activities, test and evaluation strategy, support strategy, and other periodic reporting requirements.

The PM should use existing infrastructure (e.g. internet) as appropriate and the summary in the Acquisition Strategy should briefly include leveraged and/or planned new development IDE infrastructure.

2.3.15. Life-Cycle Sustainment Planning

2.3.15.1 LCSP Executive Summary for Acquisition Strategy

DoD Directive 5000.01 requires programs to "implement performance-based logistic strategies that optimize total system availability while minimizing cost and logistics footprint". These strategies are articulated in the Life-Cycle Sustainment Plan (LCSP), documenting the Program Manager's plan for implementing these strategies throughout the life of the program. In developing the strategy the PM should invite the war fighter/user representatives and Military Service and Defense Logistics Agency logistics organizations to participate in integrated product teams.

The LCSP should describe the plan for source of repair of the major weapon system. Whenever a plan for source of repair results in a plan to award a contract for performance of maintenance and sustainment of a major weapon system, the MDA will ensure that, to the maximum extent practicable, and consistent with statutory requirements, the maintenance and sustainment contract is competitively awarded and gives full consideration to all sources (including sources that partner or subcontract with public or private sector repair activities).

The LCSP is an evolutionary document that begins in the Technology Development Phase (for approval at MS B) and provides the strategic framework for optimal sustainment at minimal LCC. It evolves into an execution plan for how sustainment is applied, measured, managed, assessed, and reported after system fielding. By Milestone C, the LCSP describes details on how the program will field and sustain the product support package necessary to meet readiness and performance objectives, lower total ownership cost, reduce risks, and avoid harm to the environment and human health.

Regardless of phase, the intent of the LCSP is to document the current program plan addressing the following major focus areas:

- The capability that will be fielded including the maintenance and support concepts along with the corresponding sustainment performance requirements
- How sustainment is being addressed as an integral part of the program's acquisition strategy and system design process
- How the sustainment metrics will be achieved and sustained throughout the life cycle
- The management approach for achieving effective and timely product support and availability throughout the life cycle
- Implementation status and strategy

Guidebook section 5.4 describes in detail the specific information that should be included in the LCSP for each life-cycle phase.

2.3.15.1. LCSP Executive Summary for Acquisition Strategy

The LCSP is a discrete document requirement beginning at milestone B and will be included in full as an appendix to the AS. Additionally an 'executive summary' of the LCSP, should be included in the main body of the AS, addressing all relevant statutory requirements and the:

- Sustainment Concepts – e.g. program support and maintenance strategy
- Sustainment Performance Requirements – including key metric, system performance indicators or any other key drivers.
- Sustainment Procurement Strategy – view of sustainment/logistics contracts and agreements to acquire the Product Support Package (including the extent to which it is traditional transaction based/process focused and performance-based/outcome focused).
- Supportability Design Characteristics – e.g. key requirements included in the system and design specifications.
- Product Support Package – e.g. the major product support elements and plan for acquiring and fielding them including the results of any Service conducted ILAs.

Special Interest Items – e.g. key technologies, initiatives or enablers the program is using in the sustainment strategy.

2.3.16. Life-Cycle Signature Support Plan

A life-cycle signature support plan (LSSP) is required for validated and approved signature dependent programs and the LSSP support requirements and funding should be included in the Acquisition Strategy. A signature dependent program is a defense acquisition that utilizes or is comprised of a sensor, system, or process that relies on signatures or signature data to successfully perform a task or mission. The LSSP should be developed during the Materiel Solution Analysis and TD Phases and matured during EMD and P&D.

The Acquisition Strategy should describe signature support requirements and required funding to support program-related efforts. The requirements and required funding should be developed in concert with the Intelligence community and the Senior Signature Management Forum.

If the LSSP needs to be classified to fulfill the information requirement it should be so noted in the unclassified Acquisition Strategy and a classified LSSP annex of the Acquisition Strategy should be handled separately. Such a classified annex may combine with the CPI/PPP summary as described in Section 2.3.12.

Applicable acquisition programs need to identify, capture, and address the signatures essential to the development, testing, fielding, operation, and maintenance of required weapons, smart munitions, sensors, and systems capabilities at each program milestone and prior to proceeding to the Low-Rate Initial Production (LRIP), production and/or fielding decision.

2.3.17. Chemical, Biological, Radiological and Nuclear Survivability

In accordance with DoDI 3150.09, CBRN survivability is a requirement of all CBRN mission-critical systems regardless of Acquisition Category. The Milestone B AS should strategically discuss the program's development plans to ensure an appropriate level of chemical, biological, radiological and/or nuclear survivability of end items at IOC and beyond. At MS C the CBRN section of the AS should be updated as appropriate, continuing to reflect IOC and beyond.

The AS should state whether the program has been designated as mission-critical and, if mission-critical, if CBRN mission-critical, including the designating authority and a brief rationale. Regardless of mission-criticality and/or CBRN mission-criticality designation, the AS should describe the program's operating environment and CBRN survivability requirements, if any. If the program has no CBRN survivability requirements, the AS should so state, and include the basis (i.e., reference the requirements/capability document). If the program has CBRN survivability requirements, the AS should provide a cross walk between the program's CBRN survivability requirements and the plan by which the requirements will be achieved and identify any special or unique test and evaluation requirements.

DoDI 3150.09 requires CBRN mission-critical systems be CBRN survivable in accordance with their capabilities documents' survivability requirements. Enclosure 3 of DoDI 3150.09 provides procedures for sponsors, materiel developers, and Milestone Decision Authorities. In the context of the Acquisition Strategy, the materiel developer should provide a cross walk between the program's CBRN survivability requirements and the plan by which the requirements will be achieved and identify any special or unique test and evaluation requirements.

2.3.18. Human Systems Integration

Per DoD Instruction 5000.02, Enclosure 8, and Guidebook Chapter 6, the PM should integrate manpower, personnel, training, human factors, safety and occupational health, personnel survivability, and habitability considerations into the acquisition process. Human Systems Integration (HSI) initiatives optimize total system performance and minimize total ownership cost.

The Acquisition Strategy should summarize how HSI requirements will be integrated within the systems engineering, logistics, technology development and resource management processes, including a summary of the HSI risks and supporting mitigation plans. The SEP should provide a more detailed description of the systems engineering process and how HSI requirements and risks are managed.

All programs should summarize their manpower goals and key technologies or design features for projected manpower savings that minimize the system's total ownership cost.

- Training: Provide an overview of the System Training Plan (STP) addressing training required for the system (including operations and maintenance) for all training locations. In addition to lesson plans, courses and training material the discussion should include the training equipment and its support.

- Manpower and Personnel

- System Operator Requirements: List the various operator specialty codes or civilian / contractor equivalent skills and requirements for system operators. Include the quantity of operators by skill category and any other special requirements for operators such as security clearance, sub-skills, and qualification certificates. List any new personnel requirements and identify any shortfalls in the manpower requirements.

- System Maintainer Requirements: List the various unit level maintainer, or civilian / contractor equivalent skills, requirements for any maintainers that will support the system (including Depot level maintainers). List the quantity of maintainers by Specialty Codes required to maintain the system, and any other special requirements for maintainers such as security clearance, sub-skills, and certificates.

- Human System Integration HSI/MANPRINT: Describe how the program office will maximize total system performance while ensuring a safe, efficient, and enhanced interaction between the user and the technical system.

2.3.19. Environment, Safety, and Occupational Health (ESOH)

The Acquisition Strategy should include a summary of the Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE).
Specifically the PESHE summary should include the following PESHE items:

- identification of ESOH responsibilities
- a strategy for integrating ESOH considerations into the systems engineering process
- a description of the method for tracking hazards throughout the life cycle of the system
- identification of ESOH risks and their mitigation status
- identification of plans for minimization and/or safe disposal of hazardous materials, wastes, and pollutants associated with the system
- a compliance schedule for National Environmental Policy Act (NEPA) (42 U.S.C. 4321-4370d and Executive Order (E.O.) 12114).

Additionally, the ESOH section of the Acquisition Strategy should address the following:

- events or proposed actions (such as, but not limited to T&E and fielding/basing activities) throughout the life cycle of the program that may require preparation of formal NEPA/EO 12114 documentation
- the anticipated initiation date for each proposed event or action
- proponent responsible for preparing the NEPA/EO 12114 documentation for each proposed event or action
- the anticipated type of NEPA/EO 12114 document (e.g., Categorical Exclusion, Environmental Assessment and Finding of No Significant Impact, Environmental Impact

Statement, Record of Decision, Overseas Environmental Assessment, and Overseas Environmental Impact Statement) which the proponent should complete prior to the proposed action start date
- the anticipated start and completion dates for the final NEPA/EO 12114 document
- the specific approval authority for the documents

DoD Instruction 5000.02, Enclosure 12, paragraph 6, establishes the DoD Component Acquisition Executive (CAE) or designee (for joint programs, the DoD CAE of the Lead Executive Component) as the approval authority for system-related NEPA/EO 12114 documentation.

The Instruction also directs the PM to integrate ESOH risk management into the overall systems engineering process for all developmental and sustaining engineering activities. As part of risk reduction, the PM should eliminate ESOH hazards where possible, and manage ESOH risks where hazards cannot be eliminated.

2.3.20. Military Equipment Valuation and Accountability (MEVA)

2.3.20. Military Equipment Valuation and Accountability (MEVA)

As a part of the Acquisition Strategy development, the PM must develop a program description that identifies contract deliverable military equipment, non-military equipment, and other deliverable items. The program description is a requirement of the Military Equipment Valuation and Accountability (MEVA) business processes.

MEVA is a DoD initiative to value, capitalize, depreciate, accurately account for, and report military equipment meeting the capitalization threshold. Prior to 2003, military equipment was classified as National Defense Property, Plant, and Equipment (PP&E).

It was expensed in the period that it was procured. In 2003, there was a change. Statement of Federal Financial Accounting Standards (SFFAS) No. 23 reclassified military equipment from National Defense PP&E to General PP&E. This reclassification meant that military equipment would no longer be treated as an expense, but rather as an asset on the Department's balance sheet.

The accounting standards for General PP&E are governed by SFFAS No. 6, which requires that we accurately account for the full cost of assets, including their capitalization and depreciation. This means, we are required to: 1) Identify the cost of Government-Furnished Material embedded in the end item and 2) Exclude the cost of items that should not be included in the value. To further facilitate this requirement, the Proper Financial Accounting treatment for

Military Equipment (PFAT4ME) Policy provides specific guidance for PMs, Business Financial Managers (BFMs), and Procurement Contracting Officers.

2.3.20.1. PFAT4ME Guidance for PMs, BFMs, and Contracting Officers

The PM for any program, project, product, or system that has deliverable end items with a unit cost at or above $100,000 (the current capitalization threshold) should prepare a program description as part of the Acquisition Strategy at Milestone C. The program description should be consistent with a level 2 work breakdown structure (WBS) as described in MIL-STD-881.

The PM should calculate the unit cost by summing the estimated cost of the end item with the estimated costs of all associated government furnished equipment, training manuals, technical data, engineering support, etc., NOT including spares and support equipment. The description should identify the following deliverables:

- the end item(s) meeting the unit cost threshold (i.e. $100,000)
- the government furnished property that will be included in the end item
- other deliverables that will accompany the end item (e.g., manuals, tech data, etc.)
- other types of deliverables that will be bought with program funding (e.g., initial spares, support equipment, special tooling and test equipment, etc.) but that cannot be directly attributed to a specific end item

The BFM uses the program description to develop a procurement request that segregates the contract deliverables based on their proper financial accounting treatment. The Procurement Contracting Officer ensures that solicitations, proposals, and contracts maintain the line item structure provided by the BFM so that proper financial accounting treatments can be applied to military equipment.

For further guidance on MEVA business processes, visit the MEVA website or receive help by completing the MEVA Support Form.

2.3.20.2. Accounting Review

The PM should provide a copy of the program description to the staff element(s) that supports the accounting transactions for the program, generically referred to here as the "accounting specialist". The accounting specialist should review the description(s) and compare them to applicable federal accounting standards (e.g., Statement of Federal Financial Accounting Standard Number 23) and financial management regulations.

If the accounting specialist determines that the program will not deliver end items that fall within applicable accounting standards/regulation criteria, no further actions are needed. However, if the accounting specialist determines that the program will deliver end items that fall within applicable accounting standards/regulation criteria (i.e., the program is a "capital" program), the

PM should include a statement in the appropriate commitment documents and contract requisitions that these documents and requisitions are part of a capital program.

2.3.21. Corrosion Prevention and Control Plan/Strategy

As part of a long-term DoD Corrosion Prevention and Control strategy that supports reduction of total cost of system ownership, each ACAT I program should document its strategy in a Corrosion Prevention and Control Plan. The Plan is only required for ACATI programs. The Plan should be included in the Acquisition Strategy at Milestones B and C, use of an appendix or annex is appropriate in this case. If the Plan proves too voluminous it may be provided separately and an executive summary take its place in the Acquisition Strategy. If this is the case the full Corrosion Prevention Control Plan document should be reference in this section of the Acquisition Strategy, with the executive summary.

Corrosion considerations should be objectively evaluated throughout program design and development activities, with trade-offs made through an open and transparent assessment of alternatives. Details of the Corrosion Prevention and Control Plan can be found in the Corrosion Prevention and Control Plan Guidebook .

2.4. Acquisition Strategies and Acquisition Plans

2.4.1. Federal Procurement Requirements

2.4.2. Distinctions for Each Requirement

2.4. Acquisition Strategies and Acquisition Plans

The Acquisition Strategy required by DoD Instruction 5000.02 is not the same as the acquisition plan required by FAR Subpart 7.1 and DFARS Subpart 207.1. The Acquisition Strategy is a top-level description, in sufficient detail to allow decision-makers and the milestone decision authority (MDA) to assess whether the strategy makes good business sense, effectively implements laws and policies, and reflects management's priorities. Once approved by the MDA, the Acquisition Strategy provides a basis for more detailed planning.

2.4.1. Federal Procurement Requirements

The FAR requires acquisition planning for all Federal procurements, and the DFARS requires PMs to prepare written Acquisition Plans (APs) for most acquisitions exceeding $10 million. APs are execution-oriented and tend to contain more contracting-related detail than an Acquisition Strategy. An AP normally relates to a singular contractual action, whereas an Acquisition Strategy covers the entire program and may reflect the efforts of multiple contractual actions.

2.4.2. Distinctions for Each Requirement

Because both the DoD Instruction 5000.02 requirement for an Acquisition Strategy and the FAR/DFARS requirement for an AP apply to program planning, there are understandably questions about how they differ and how they relate to each other.

There is no DoD-level rule that precludes the PM from preparing a single document to satisfy both requirements; in fact, FAR 34.004 dealing with major systems acquisition requires that the Acquisition Strategy "qualify" as the AP. However, DoD Components often prefer to provide a more general Acquisition Strategy to the MDA for approval and choose to prepare a separate, more detailed AP. If a separate AP is written, the AP may not be approved until after the Acquisition Strategy has been approved.

The distinctions between the requirement for the Acquisition Strategy and the requirement for the AP are summarized in table 2.4.2.F1

	ACQUISITION STRATEGY	ACQUISITION PLAN
Required by	DoD Instruction 5000.02, Enclosure 2, paragraphs 5(c) and 6(a)	FAR 7.1
Required for	All acquisition categories	Contracting or procuring for development activities when the total cost of all contracts for the acquisition program is estimated at $10 million or more; procuringproducts or services when the total cost of all contracts is estimated at $50 million or more for all years or $25 million or more for any one fiscal year; and other procurements considered appropriate by the agency.
Approval Authority	MDA	Component Acquisition Executive or designee in accordance with Agency FAR supplements.
Purpose	Describes overall strategy for managing the acquisition program. The	Comprehensive plan for implementing the contracting strategy.

	Acquisition Strategy describes the PM's plan to achieve programmatic goals and summarizes the program planning and resulting program structure.	
Use	Required at program initiation. The Acquisition Strategy should be updated for all subsequent milestones, at the full-rate production decision review, and whenever the approved strategy changes.	Integrates the efforts of all personnel responsible for significant aspects of the contractual agreement. The purpose is to ensure that the Government meets its needs in the most effective, economical, and timely manner.
Level of Detail	Strategy level. Needed by MDA for decision-making. Also planning level for some discrete information requirements.	Execution level. Provides the detail necessary to execute the approach established in the approved acquisition strategy and to guide contractual implementation and conduct acquisitions.
Content	Prescribed by DoD Instruction 5000.02; additional guidance in the Defense Acquisition Guidebook	Prescribed by FAR 7.1; DFARS 207
Individual Responsible for Preparing the Document	PM	Person designated as responsible.

Table 2.4.2.F1. Summary of Distinctions between the Acquisition Strategy and Acquisition Plan

DEFENSE ACQUISITION GUIDEBOOK
Chapter 3 -- Affordability and Life-Cycle Resource Estimates

3.0. Overview

3.0.1. Purpose

This chapter addresses acquisition program affordability and resource estimation. It provides explanations of the relevant program and pre-program activities and information required by DoD Instruction 5000.02, *Operation of the Defense Acquisition System*, and discusses the associated support provided by the appropriate Office of the Secretary of Defense staff elements.

DoD Instruction 7000.14 establishes DoD 7000.14-R as the DoD-wide financial management Regulation to be used by all DoD Components for accounting, budgeting, finance, and financial management education and training. The link to the "FMR" is provided as a convenience to the reader.

3.0.2. Contents

Section 3.1 provides introductory background material intended for a general audience. It describes the concept of program life-cycle cost, and provides definitions of terms used by the DoD cost community. It also introduces the concepts of total ownership cost, and fully burdened cost of delivered energy.

The next five sections are more specialized; they discuss the specific milestone review procedures, expectations, and best practices for a variety of topics related to acquisition program affordability, cost, and manpower:

Section 3.2 describes the basic policies associated with the consideration of affordability in the acquisition process, and offers one possible analytic approach to the preparation of affordability assessments. This section also explains the Department's full-funding policy, and describes the concept known as Cost as an Independent Variable.

Section 3.3 describes the Analysis of Alternatives process.

Section 3.4 describes the role of both DoD Component cost estimates, and independent cost estimates, in support of the DoD acquisition system.

Section 3.5 describes the review procedures for manpower estimates.

Section 3.6 discusses procedures unique to economic analyses of major automated information systems.

The last section, 3.7, is intended for less experienced cost analysts working in the acquisition community. This section, which is tutorial in nature, provides a recommended analytic approach for preparing a life-cycle cost estimate for a defense acquisition program.

3.1. Life-Cycle Costs/Total Ownership Costs

3.1.1. Introduction

Both DoD Directive 5000.01, *The Defense Acquisition System*, and DoD Instruction 5000.02, *Operation of the Defense Acquisition System*, make reference to life-cycle cost and total ownership cost. This section of the Guidebook explains the meaning for each of these terms. The terms are similar in concept, but somewhat different in scope and intent. For a defense acquisition program, life-cycle cost consists of research and development costs, investment costs, operating and support costs, and disposal costs over the entire life cycle. These costs include not only the direct costs of the acquisition program, but also include indirect costs that would be logically attributed to the program. In this way, all costs that are logically attributed to the program are included, regardless of funding source or management control.

The concept of total ownership cost is related, but broader in scope. Total ownership cost includes the elements of life-cycle cost, as well as other infrastructure or business process costs not normally attributed to the program. Section 3.1.5 defines and describes this concept in more detail.

Program cost estimates that are supporting the defense acquisition system normally are focused on life-cycle cost or elements of life-cycle cost. Examples of such cases where cost estimates support the acquisition system include Affordability Assessments, establishment of program cost goals for Acquisition Program Baselines, Independent Cost Estimates, or estimates of budgetary resources. However, for programs in Pre-Systems Acquisition or the Engineering and Manufacturing Development Phase, cost estimates that are used within the program office to support system trade-off analyses-such as evaluations of design changes, or assessments of energy efficiency, reliability, maintainability, and other supportability considerations-may need to be broader in scope than traditional life-cycle cost estimates to support the purpose of the analyses being conducted. Moreover, for mature programs (in transition from production and deployment to sustainment), cost estimates in many cases may need to be expanded in scope to embrace total ownership cost concepts in order to support broad logistics or management studies.

3.1.2. Life-Cycle Cost Categories and Program Phases

DoD 5000.4-M, DoD Cost Analysis Guidance and Procedures, provides standardized definitions of cost terms that in total comprise system life-cycle costs. Life-cycle cost can be defined as the sum of four major cost categories, where each category is associated with sequential but overlapping phases of the program life cycle. Life-cycle cost consists of

1. research and development costs associated with the Materiel Solution Analysis phase, the Technology Development phase, and the Engineering and Manufacturing Development phase,
2. investment costs associated with the Production and Deployment phase,
3. operating and support costs associated with the sustainment phase, and
4. disposal costs occurring after initiation of system phase out or retirement, possibly including demilitarization, detoxification, or long-term waste storage.

Figure 3.1.2.F1 depicts a notional profile of annual program expenditures by cost category over the system life cycle.

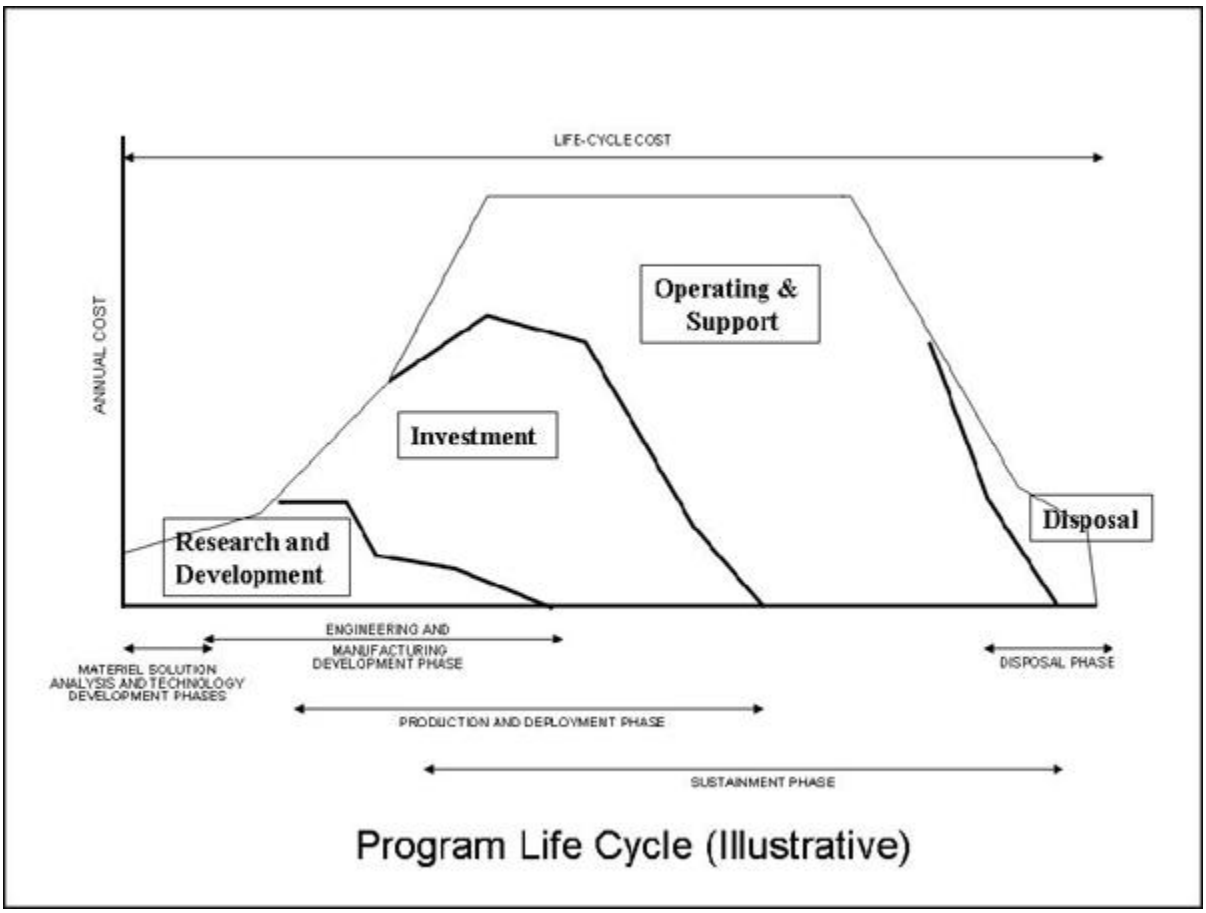


Figure 3.1.2.F1. Illustrative Program Life Cycle

3.1.3. Life-Cycle Cost Category Definitions

The following sections summarize the primary cost categories associated with each program life-cycle phase.

3.1.3.1. Research and Development Costs

Research and Development consists of development costs (both contractor and Government) incurred from the beginning of the materiel solution analysis phase through the end of the Engineering and Manufacturing Development (EMD) Phase (excluding costs associated with Low-Rate Initial Production). This typically includes costs of materiel solution trade studies and advanced technology development; system design and integration; development, fabrication, assembly, and test of hardware and software for prototypes and/or engineering development

models; system test and evaluation; systems engineering and program management; and product support elements associated with prototypes and/or engineering development models.

Research and Development costs are estimated and presented using the following categories:
Materiel Solution Analysis Phase
Technology Development Phase

[Note: For those programs with extensive prototyping and/or preliminary design activities that occur before Milestone B, the Technology Development Phase should be expanded with lower level cost categories, similar to the categories used in the EMD Phase]

Engineering and Manufacturing Development Phase:
Prime Mission Product
System Test and Evaluation
Systems Engineering/Program Management
Engineering Change Orders
Peculiar Support Equipment
Common Support Equipment
Training
Technical Publications and Data
Initial Spares and Repair Parts
Industrial Facilities
Operational/Site Activation

Complete definitions and further details are provided throughout MIL-STD-881, *Work Breakdown Structures for Defense Materiel Items*. Note the following:

- The Standard expands the Prime Mission Product category into more detailed elements, and these lower level elements vary by product commodity (such as aircraft, electronic system, missile system, sea system, or surface vehicle)
- Supportability analysis that defines the requirements for the logistics elements is part of Systems Engineering, and planning and management associated with the logistics elements is part of Program Management
- In most cost estimates, the Engineering Change Orders element is added to the Standard taxonomy to allow a contingency for design or other scope changes
- In most cost estimates, the first four EMD elements shown above are subtotaled and displayed as Flyaway (or Rollaway, Sailaway, or other similar term). The remaining EMD elements are often grouped together and labeled as "Acquisition Logistics", "Product Support Package", or other similar term
- The Training element includes training equipment and devices, training course materials, and training services
- Specialized facilities (fixtures, test chambers, laboratories, etc) are considered part of the Work Breakdown Structure (WBS) element that they support. General brick and mortar type facilities are part of the Industrial Facilities element

- Specialized contractor support is considered part of the WBS element that it supports. Contractor support associated with the service, maintenance or launch of prime mission systems is part of the Operational/Site Activation element

An abbreviated version of the above format is used in Budget Exhibit R-3, RDT&E Project Cost Analysis, to display budget justifications and financial reporting for Research, Development, Test and Evaluation (RDT&E) projects with budgets greater than $1 million in either budget year. (See DoD 7000.14 R, Financial Management Regulation, Volume 2B, Chapter 5.)

3.1.3.2. Investment Costs

Investment consists of production and deployment costs incurred from the beginning of low rate initial production through completion of deployment. This typically includes procurement costs associated with producing and deploying the primary hardware; systems engineering and program management; product support elements associated with production assets; military construction; and operations and maintenance associated with the production and deployment phase.

Investment costs are estimated and presented using the following categories:

Procurement:
Prime Mission Product
System Test and Evaluation (if applicable)
Systems Engineering/Program Management
Engineering Change Orders
Peculiar Support Equipment
Common Support Equipment
Training
Technical Publications and Data
Initial Spares and Repair Parts
Industrial Facilities
Operational/Site Activation
Military Construction
Operations and Maintenance (acquisition-related during production and deployment)

Complete definitions and further details for the Procurement elements are provided throughout MIL-STD-881, *Work Breakdown Structures for Defense Materiel Items*.

Note the following:

- The Standard expands the Prime Mission Product category into more detailed elements, and these lower level elements vary by product commodity (such as aircraft, electronic system, missile system, sea system, or surface vehicle)

- Supportability analysis that defines the requirements for the logistics elements is part of Systems Engineering, and planning and management associated with the logistics elements is part of Program Management
- In most cost estimates, the Engineering Change Orders element is added to the Standard taxonomy to allow a contingency for design or other scope changes
- In most cost estimates, the first four procurement elements shown above are subtotaled and displayed as Flyaway (or Rollaway, Sailaway, or other similar term). The remaining procurement elements are often grouped together and labeled as "Acquisition Logistics", "Product Support Package", or other similar term
- The Training element includes training equipment and devices, training course materials, and training services
- Specialized facilities (fixtures, test chambers, laboratories, etc) are considered part of the Work Breakdown Structure (WBS) element that they support. General brick and mortar type facilities are part of the Industrial Facilities element
- Specialized contractor support is considered part of the WBS element that it supports. Contractor support associated with the service, maintenance or launch of prime mission systems is part of the Operational/Site Activation element

An abbreviated modified version of the above format (procurement only) is used in Budget Exhibit P-5, Cost Analysis, to display budget justifications and financial reporting for procurement programs with budgets greater than or equal to $5 million in either budget year. (See DoD 7000.14 R, Financial Management Regulation, Volume 2B, Chapter 4.)

3.1.3.3. Operating and Support (O&S) Costs

O&S consists of sustainment costs incurred from the initial system deployment through the end of system operations. This includes all costs of operating, maintaining, and supporting a fielded system. Specifically, this consists of the costs (organic and contractor) of manpower, equipment, supplies, software, and services associated with operating, modifying, maintaining, supplying, training, and supporting a system in the DoD inventory. This includes costs directly and indirectly attributable to the system (i.e., costs that would not occur if the system did not exist), regardless of funding source or management control. Direct costs refer to the resources immediately associated with the system or its operating unit. Indirect costs refer to the resources that provide indirect support to the system (including its manpower or facilities). For example, the pay and allowances for a unit-level maintenance technician would be treated as a direct cost, but the cost of medical support for the same technician would be an indirect cost.

Operating and Support costs are estimated and presented using the following categories:

Unit-Level Manpower
Operations Manpower
Unit-Level Maintenance Manpower
Other Unit-Level Manpower
Unit Operations

Operating Materiel
Energy (Fuel, Electricity, etc.)
Training Munitions and Expendable Stores
Other Operational Materiel
Support Services
Temporary Duty
Maintenance
Organizational Maintenance and Support
Intermediate Maintenance
Depot Maintenance
Sustaining Support
System Specific Training
Support Equipment Replacement
Operating Equipment Replacement
Sustaining Engineering and Program Management
Other Sustaining Support
Continuing System Improvements
Hardware Modifications or Modernization
Software Maintenance and Modifications
Indirect Support
Installation Support
Personnel Support
General Training and Education

Further details and complete definitions are provided in the Operating and Support Cost-Estimating Guide promulgated by the OSD Director, Cost Assessment and Program Evaluation (DCAPE).

3.1.3.4. Disposal Costs

Disposal consists of costs associated with demilitarization and disposal of a military system at the end of its useful life. It is important to consider demilitarization and disposal early in the life cycle of a system because these costs can be significant, depending on the characteristics of the system. Costs associated with demilitarization and disposal may include disassembly, materials processing, decontamination, collection/storage/disposal of hazardous materials and/or waste, safety precautions, and transportation of the system to and from the disposal site. Systems may be given credit in the cost estimate for resource recovery and recycling considerations.

The intent of the use of the disposal cost category is to ensure that design and other decisions made early in the program consider their effects on the specific long-term disposal costs that can be logically attributed to the program. Disposal costs of a more general nature, such as the removal of unexploded ordnance at a training range, would normally not be attributed to a specific aircraft program that in the future may participate in training exercises at that range.

Disposal costs may be estimated and presented using the following categories, subject to tailoring for the circumstances unique to each program:
Removal from Active Service
Demilitarization
Removal and Disposal of Hazardous Materials
Reclamation of Parts
Storage
Final Disposal or Salvage

3.1.4. Implications of Evolutionary Acquisition

The application of life-cycle cost categories to program phases may need to be modified for programs with evolutionary acquisition strategies. DoD Instruction 5000.02, *Operation of the Defense Acquisition System*, Enclosure 2, paragraph 2, describes the evolutionary acquisition approach for acquisition programs. In an evolutionary approach, the ultimate capability delivered to the user is provided in increasing increments. Evolutionary acquisition strategies (1) define, develop, produce and deploy an initial, militarily useful capability (Increment 1) based on proven technology, demonstrated manufacturing capabilities, and time-phased definition capabilities needs; and (2) plan up front for subsequent development, production and deployment of increments beyond the initial capability over time (Increments 2 and beyond).

For a program with evolutionary acquisition, the question often arises concerning the scope of the life-cycle cost estimate presented at a milestone review. Although the situation may vary somewhat depending on individual circumstances, the life-cycle cost estimate should attempt to address as much of the program, including known future increments, as can be defined at the time of the initial (Increment 1) milestone review. Any exclusions (for portions of the program that cannot be defined at that time) should be clearly identified.

The application of life-cycle cost categories and program phases (as described in section 3.1.2) may need to be modified to account for the evolutionary acquisition strategy. Figure 3.1.4.F1 depicts a notional profile of annual program expenditures by cost category for a program with evolutionary acquisition.

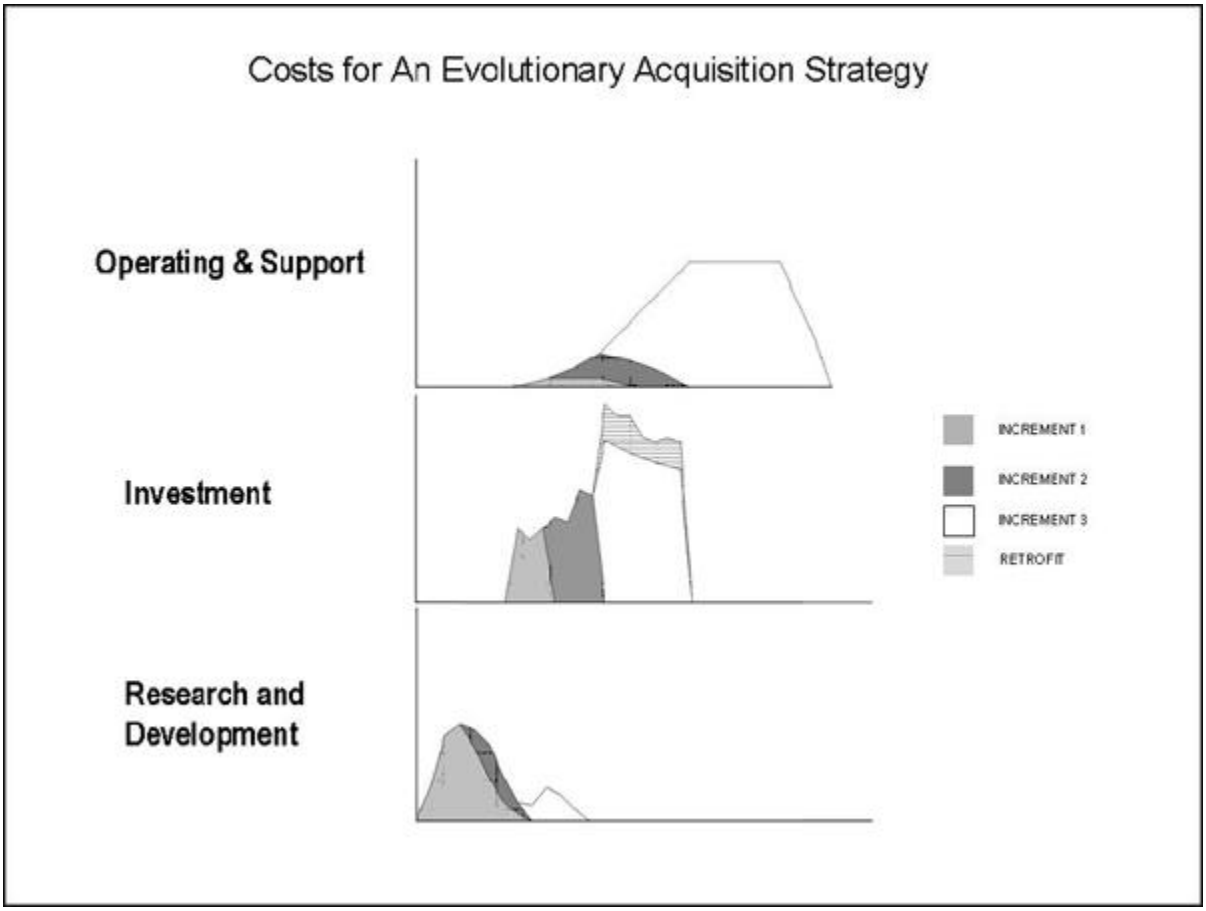


Figure 3.1.4.F1. Illustrative Program Life Cycle under Evolutionary Acquisition

3.1.5. Total Ownership Costs

As explained earlier, total ownership cost includes the elements of a program's life-cycle cost, as well as other related infrastructure or business processes costs not necessarily attributed to the program in the context of the defense acquisition system. Infrastructure is used here in the broadest possible sense, and consists of all military department and defense agency activities that sustain the military forces assigned to the combatant and component commanders. Major categories of infrastructure are support to equipment (acquisition and central logistics activities), support to military personnel (non-unit central ["school-house"] training, personnel administration and benefits, and medical care), and support to military bases (installations and communications/information infrastructure).

In general, traditional life-cycle cost estimates are often adequate in scope to support the review and oversight of cost estimates made as part of the acquisition system. However, in special cases, depending on the issue at hand, the broader perspective of total ownership cost may be more appropriate than the life-cycle cost perspective, which may be too narrow to deal with the

particular context. As discussed previously, for a defense acquisition program, life-cycle costs include not only the direct costs of the program, but also include certain indirect costs that would be logically attributed to the program. In a typical life-cycle cost estimate, however, the estimated indirect costs would include only the costs of infrastructure support specific to the program's military manpower (primarily medical support and system-specific training) and the program's associated installations or facilities (primarily base operating support and facilities sustainment, restoration and modernization).

Many other important support or infrastructure activities (such as recruiting and accession training of new personnel, individual training other than system-specific training, environmental and safety compliance, contract oversight support from the Defense Contract Management Agency and the Defense Contract Audit Agency, and most management headquarters functions) are normally not considered in the scope of a traditional acquisition program life-cycle cost estimate. In addition, important central (i.e., wholesale) logistics infrastructure activities such as supply chain management are implicitly incorporated in a traditional life-cycle cost estimate, but their costs are somewhat hidden (because these costs are reflected in the surcharges associated with working capital fund arrangements and are not explicitly identified). However, there could easily be cases where explicit consideration of such infrastructure activities would be important and would need to be recognized in a cost estimate or analysis. Examples of such cases are cost analyses tied to studies of alternative system support concepts and strategies; reengineering of business practices or operations; environment, safety, and occupational health considerations; or competitive sourcing of major infrastructure activities. In these cases, the traditional life-cycle cost structure may not be adequate to analyze the issue at hand, and the broader total ownership cost perspective would be more appropriate. For such instances, the typical life-cycle cost tools and data sources would need to be augmented with other tools and data sources more suitable to the particular issue being addressed.

One special case of where traditional life-cycle cost models and data sources need to be augmented concerns the inclusion of the fully burdened cost of delivered energy in trade-off analyses for certain tactical systems. This case is discussed in the next section.

3.1.6. Fully Burdened Cost of Delivered Energy

Inefficient use of energy in tactical systems has many significant but unrecognized liabilities. It results in operational constraints and significant force protection challenges. Conversely, reductions in energy demand improve operational flexibility and reduce dependence on logistics forces. One cause for this lack of recognition is that the DoD acquisition process undervalues the benefits of technologies that can reduce energy demands by deployed systems. To remedy this, DoD has adopted the policy to apply the concept known as fully burdened cost of delivered energy for trade-off analysis conducted for all operational (or "tactical") systems with end items that create a demand for delivered energy (see DoD Instruction 5000.02, Enclosure 7, paragraph 6). This policy applies to all military systems that may be employed in military operations. Vehicles such as buses or cars used in support of routine base operations normally would not be regarded as "tactical."

For tactical systems with delivered energy requirements, the Analysis of Alternatives conducted during the Materiel Solution Analysis phase shall include an estimate of the fully burdened cost of delivered energy, added to the total ownership cost estimate, to help guide system design and technology trades (see DoD Instruction 5000.02, Enclosure 7, paragraphs 5.f.(2)). Further explanation of the concept and the methodology that should be used to make this estimate can be found in the paper "Fully Burdened Cost of Delivered Energy-Methodological Guidance for Analyses of Alternatives and Acquisition Tradespace Analysis."

3.2. Affordability

3.2. Affordability

DoD Directive 5000.01 provides the fundamental acquisition policies for cost and affordability and program stability. Affordability can be defined as the degree to which the life-cycle cost of an acquisition program is in consonance with the long-range modernization, force structure, and manpower plans of the individual DoD Components, as well as for the Department as a whole. The remainder of this section discusses different aspects of affordability. Section 3.2.1 describes how affordability is considered during the identification of military capability needs, and at acquisition milestone reviews. Section 3.2.2 provides some recommended analytic approaches to

the preparation of affordability assessments. Section 3.2.3 explains the Department's full-funding policy. And section 3.2.4 describes a process known as Cost As an Independent Variable, which can be used to ensure that life-cycle cost has equal consideration with performance and schedule in program decisions.

3.2.1. Affordability Considerations

Affordability plays an important part in program decisions throughout the life cycle. Even before a program is approved for formal initiation into the systems acquisition process, affordability plays a key role in the identification of capability needs. Program affordability is part of the Joint Capabilities Integration and Development System, which balances cost versus performance in establishing Key Performance Parameters. Moreover, all elements of life-cycle cost (or total ownership cost, if applicable) are documented as part of the Capability Development Document and the Capability Production Document (section 16 in both documents). To ensure the program is affordable, cost goals are established in terms of thresholds and objectives to provide flexibility for program evolution and to support further Cost-As-an-Independent-Variable and other system performance and program schedule-related trade-off studies.

For Major Defense Acquisition Programs at Milestone B, the Milestone Decision Authority (MDA) must certify in writing to the Congress that the program is affordable,and that the Director of Cost Assessment and Program Evaluation (DCAPE) concurs with reasonable cost and schedule estimates to execute the program development and production plans. Other certification criteria are listed under 10 U.S.C. 2366b. For all acquisition programs, the MDA normally considers program affordability at all major decision points. In part, this consideration ensures that sufficient resources (funding and manpower) are programmed and budgeted to execute the program acquisition strategy. The MDA also examines the realism of projected funding over the programming period and beyond, given likely DoD Component resource constraints. To support this determination, the DoD Components or the OSD staff may be called upon to conduct Affordability Assessments. The Affordability Assessment is discussed in the next section.

3.2.2. Affordability Assessments

DoD Instruction 5000.02, Enclosure 4, Table 3, requires Affordability Assessments for all acquisition programs at Milestones B and C. The purpose of the assessment is to demonstrate that the program's projected funding and manpower requirements are realistic and achievable, in the context of the DoD Component's overall long-range modernization plan. Normally, this assessment requires a DoD Component (or even DoD-wide) corporate perspective, and so the Affordability Assessment should not be prepared by the program manager. Rather, the assessment typically should be conducted by resource analysts in the DoD Component headquarters or a supporting organization, or alternatively in the OSD staff. For a joint program, the Affordability Assessment may be prepared by the lead DoD Component, although it may be necessary to display separate analyses for each DoD Component, as appropriate.

The approach to the Affordability Assessment can vary, depending on the nature of the program and its milestone decision. This version of the Guidebook offers two possible approaches. The first approach involves analysis of the program's projected annual funding. The second approach involves simple unit-cost comparisons, calculated on a normalized life-cycle cost basis, between the current program and one or more appropriate predecessor programs.

3.2.2.1. Affordability Assessments-Projected Annual Funding

With the projected annual funding approach, the Affordability Assessment should address program funding and manpower requirements over the six-year programming period, and several years beyond. The assessment also should show how the projected program funding and manpower fits within the overall DoD Component plan, or total DoD-wide plan, for modernization, force structure, and manpower. Usually, the overall long-range plan will be broken out across the DoD Component (or DoD-wide) mission areas. The assessment then should use this information to examine, for the acquisition program's mission area, the projected funding and manpower demands, as a percentage of the DoD Component's total funding and manpower. The assessment should highlight those instances where the mission area's projected funding or manpower exceeds zero real growth from the last year of the six-year programming period, or those instances where the relative share of the DoD Component's total funding and manpower devoted to the mission area exceeds historical averages. For the instances highlighted, the assessment should provide details as to how excess funding or manpower demands will be accommodated, perhaps by reductions in modernization for other mission areas, or in other (i.e., non-modernization) accounts.

To illustrate the projected annual funding approach, the next four sections provide a notional example of the type of analyses that could be incorporated in an Affordability Assessment. This example follows a four-step process, each step of which is described below. Although this example only addresses modernization funding, the approach for sustainment funding and manpower would be similar.

3.2.2.1.1. Affordability Assessments-Notional Example (Step One)

In this hypothetical example, a major defense acquisition program is nearing Milestone B approval. For discussion purposes, this program arbitrarily is assumed to be a mobility program. A first step in the program's affordability assessment is to portray the projected annual modernization funding (RDT&E plus procurement, measured as total obligation authority, or TOA) in constant dollars for the six-year programming period, and, in addition, for an additional twelve years beyond that. Similar funding streams for other acquisition programs in the same mission area (in this example, mobility) also would be included. Figure 3.2.2.1.1.F1 is a sample chart for this first step. In this example, the acquisition program nearing milestone approval is labeled "Mobility MDAP #3." Funding also is shown for the other modernization programs in the same mission area, consisting of three other major defense acquisition programs, three other (Acquisition Category II) programs, and one miscellaneous category for minor procurement. In this example, there appears to be a significant modernization bow wave beginning around 2018,

which would then be subject to further analysis and discussion in the assessment. The term "bow wave" refers to a requirement for excess modernization funds during a period beyond the programming period, resulting from acquisition decisions made earlier. Note that the chart provides a black arrow (labeled "0% REAL GROWTH") that indicates a benchmark for the projected funding, using a straight-line extrapolation from the funding in the last year of the six year programming period.

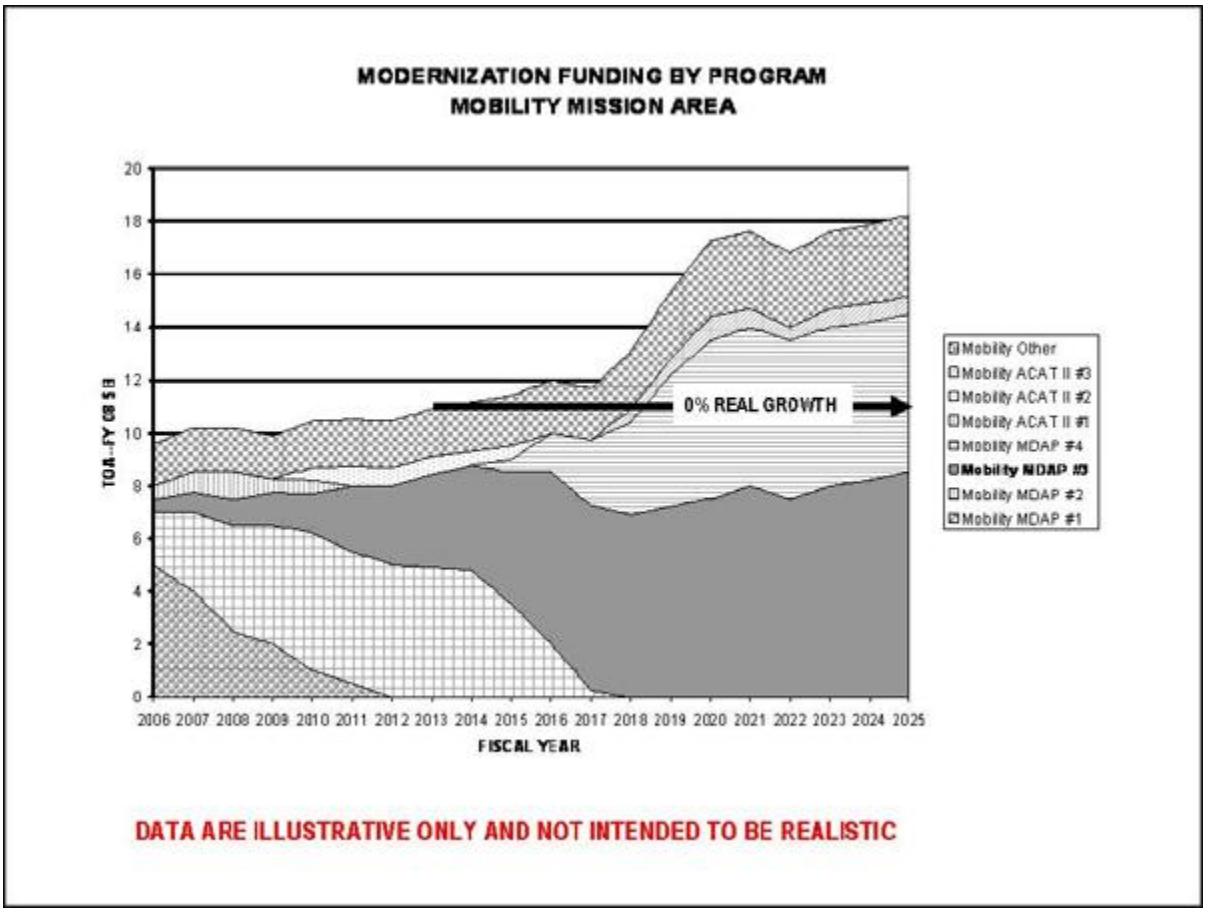


Figure 3.2.2.1.1.F1. Sample Chart of Funding Streams by Program

3.2.2.1.2. Affordability Assessments-Notional Example (Step Two)

The second step in this assessment is to portray DoD Component modernization funding stratified by mission areas, rather than by individual program. Figure 3.2.2.1.2.F1 shows a notional example of this second step. The choice of mission areas will vary depending upon circumstances. Clearly, an analysis by an individual DoD Component would portray funding only for applicable mission areas. Also, for a DoD Component like the Army, where almost all of its modernization funding is in a single mission area (Land Forces), the mission area should be

further divided into more specialized categories (such as brigade combat teams, combat aviation, maneuver enhancement, sustainment, etc.).

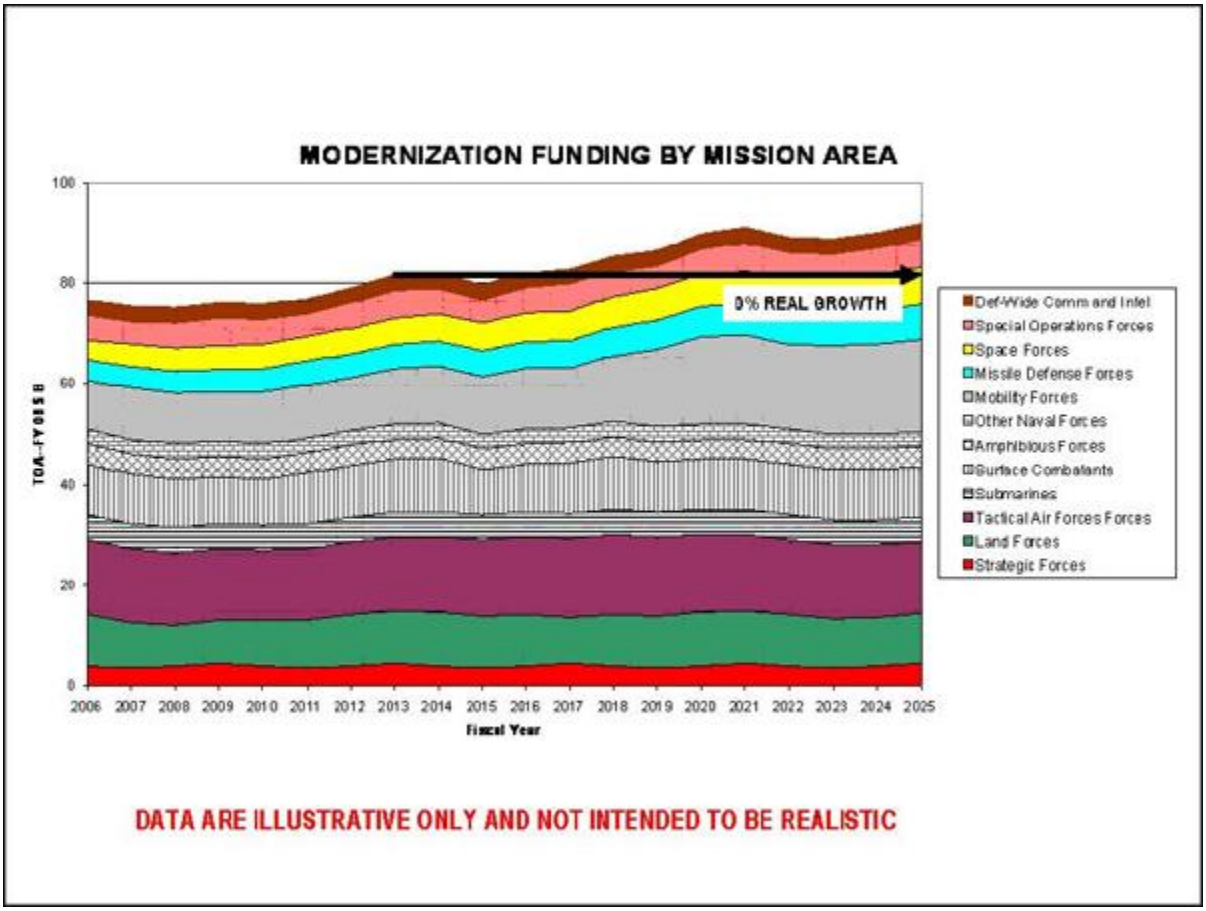


Figure 3.2.2.1.2.F1. Sample Chart of Funding Streams by Mission Area

For this example, Figure 3.2.2.1.2.F1 shows funding growth in three mission areas (space, missile defense, and mobility). What remains to be determined is whether this projected growth is realistically affordable relative to the DoD Component's most likely overall funding (top-line).

3.2.2.1.3. Affordability Assessments-Notional Example (Step Three)

The third step in this assessment is to portray the annual modernization funding, again stratified by mission areas, but measured as a percentage of the DoD Component's assumed top-line. The results are provided in Figure 3.2.2.1.3.F1.

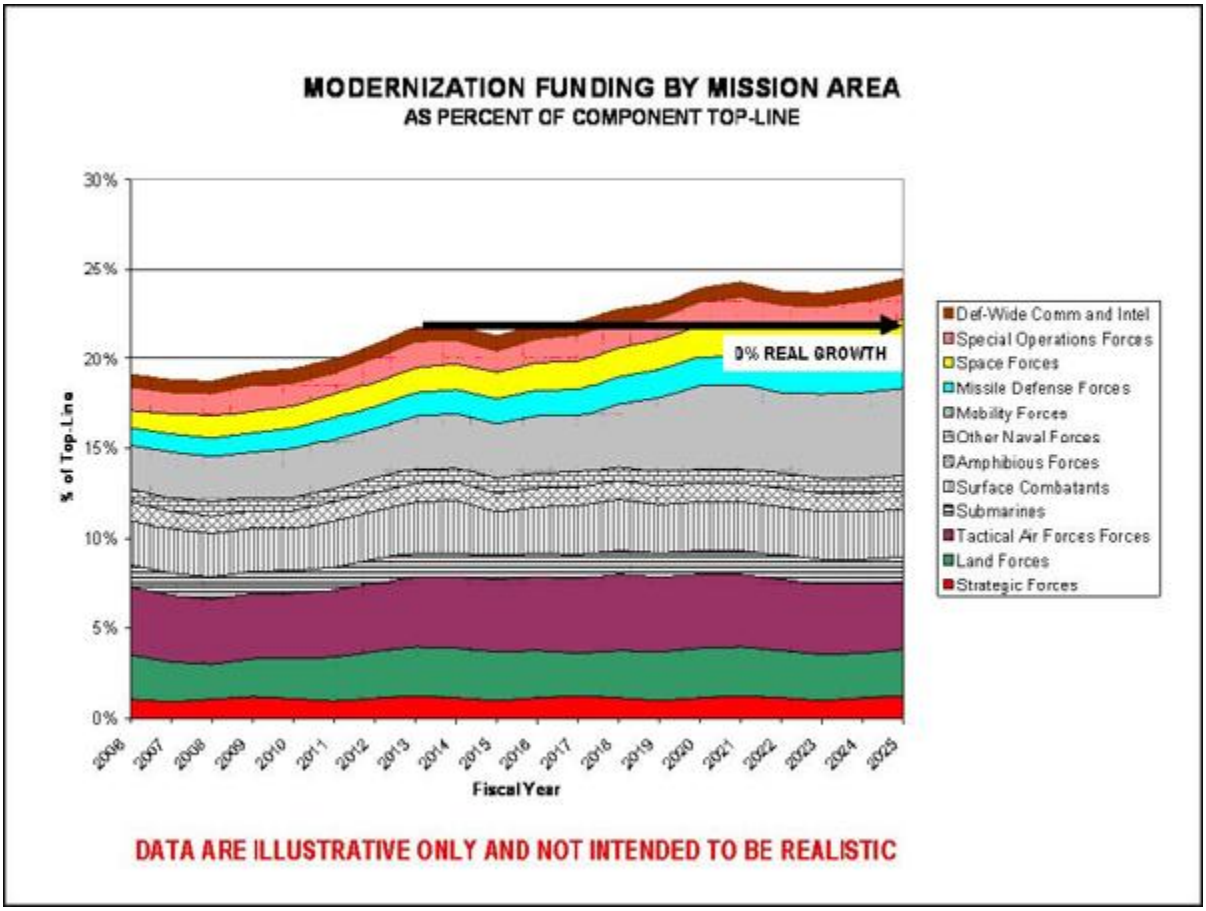


Figure 3.2.2.1.3.F1. Sample Chart of Percentage Funding by Mission Area

3.2.2.1.4. Affordability Assessments-Notional Example (Step Four)

The fourth step in this assessment is to portray the DoD Component annual modernization funding, expressed as a percentage of the projected funding top-line, as shown in Figure 3.2.2.1.4.F1. There are three distinct time periods considered in this figure. The first is a twelve-year historical period, the second is the six-year programming period, and the third is the twelve-year projection beyond the programming period. What this chart shows for this example is that the assumed mobility programs are projected to require a significantly higher share of DoD Component funding in the years beyond the programming period. In such a circumstance, the DoD Component would be expected to rationalize or justify this projected funding growth as realistic (by identifying offsets in modernization for other lower priority mission areas, or perhaps identifying savings in other accounts due to business process improvements or reforms).

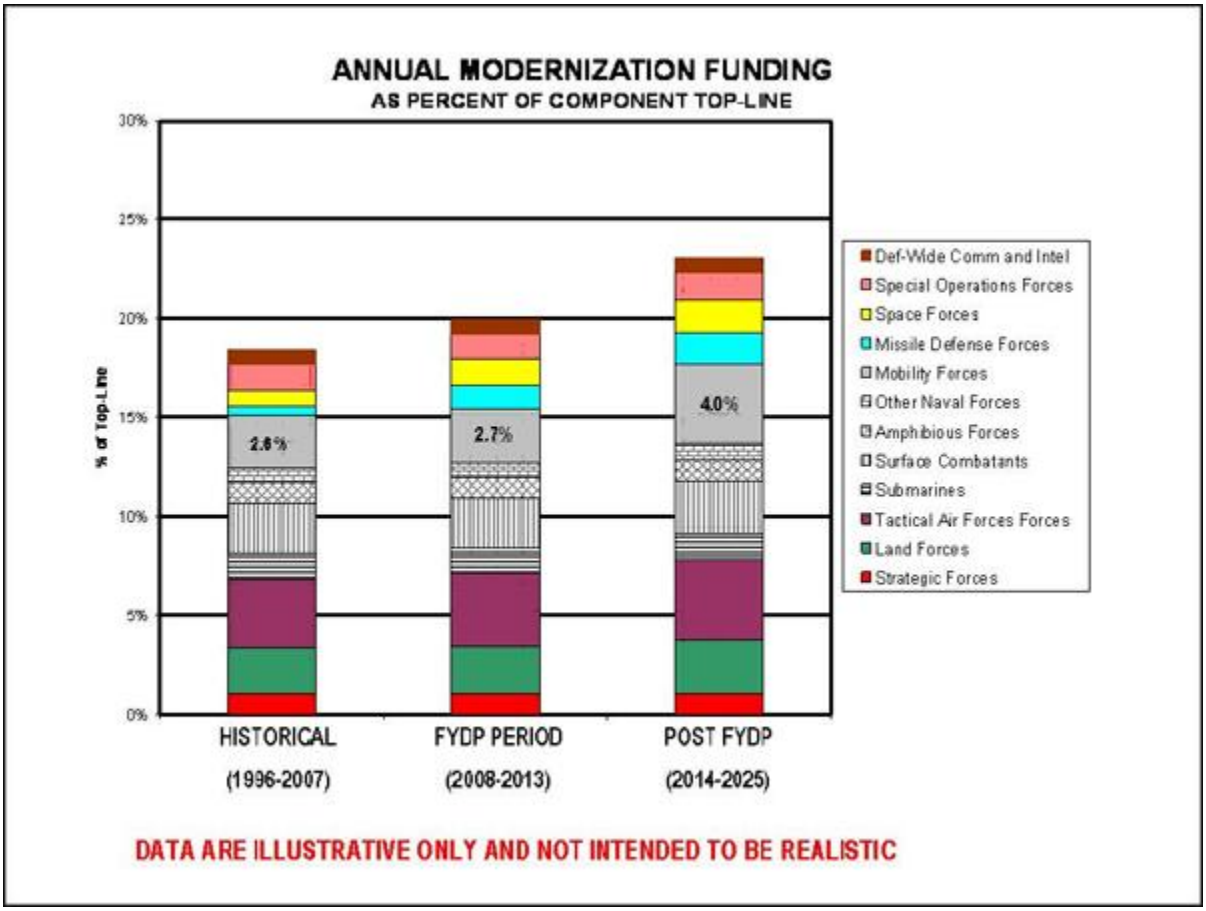


Figure 3.2.2.1.4.F1. Sample Annual Modernization Funding

The approach used in this example would need to be modified for a major automated information system, since, most likely, the mission areas associated with weapon systems would not apply. An alternative would be to portray automated information system modernization funding by joint warfighting capability area or business domain (logistics, accounting and finance, human resources management, etc.).

3.2.2.2. Affordability Assessments-Unit Cost Approach

The first approach to the Affordability Assessment, as described in the earlier sections, considers total projected annual funding, and not the unit cost of individual systems. However, it may also be desirable to assess affordability in a somewhat different way by considering the unit cost of individual systems as well. Note that for Major Defense Acquisition Programs at Milestone B, the Milestone Decision Authority must certify in writing to the Congress that the program is affordable:

1. when considering the ability of the Department of Defense to accomplish the program's mission using alternative systems;
2. when considering the per unit cost and the total acquisition cost in the context of the total resources available…;

See 10 U.S.C. 2366b for all of the Milestone B certification criteria.

To assess a program's affordability on a unit-cost basis, a common approach is to compare the unit cost of the proposed program to the unit cost of an earlier predecessor program with a similar mission. In some cases, the proposed program is a direct replacement for the predecessor program upon its retirement. A sample computation using this approach for a hypothetical airlift aircraft program is provided in Table 3.2.2.2.T1.

Nominal Example of "Unit-Cost" Approach to the Affordability Assessment

	C-X (New System)	C-Y (Legacy System)
Cost Comparison Factors:		
Unit Procurement Cost	175.0	75.0
Annual O&S Cost per System	5.8	3.8
Capacity (or Capability) Score	0.060	0.024
Equivalency Index	1.0	2.5
Unit Procurement Cost (normalized to equal capacity)	175.0	187.5
Annual O&S Cost per System (normalized to equal capacity)	5.8	9.4

All costs are FY 08 $ in millions

Table 3.2.2.2.T1. Affordability Assessment on Unit-Cost Basis

In the above example, the proposed program is labeled as the "C-X", and the predecessor program is labeled as the "C-Y". The first two rows compare the unit procurement cost and the annual Operating and Support (O&S) cost per system for the two programs. In this case, although the proposed program is considerably more expensive than the predecessor program on a unit-cost basis, it also provides more capability per system.

In such cases, it is common to compare the two programs on an equal capability basis as well as simple unit cost. In this example, which uses airlift aircraft, the capability per system "score" is measured as the system cargo-carrying capacity, expressed in million ton-miles per day. For airlift aircraft, the capacity is computed by a formula that considers the aircraft speed, payload, utilization rate, and other miscellaneous factors. For other types of systems, other metrics of capability would be more appropriate. Such metrics are usually derived from the program's Analysis of Alternatives or similar cost-effectiveness analysis.

Given some kind of capability score, it is then possible to compute the equivalency in system quantity between the proposed program and the predecessor program. In this example, a single C-X system is equivalent to 2.5 C-Y systems. Given this equivalency, the last two rows in the table compare the unit procurement cost, and the annual O&S cost per system, for the proposed program, compared to an equivalent number (in this case, 2.5) of the predecessor program.

3.2.2.3. Affordability Assessments-Other Remarks

It is desirable to conduct sensitivity analyses and other excursions as part of the Affordability Assessment. The sensitivity analysis might address the effect of different cost estimates or programmatic assumptions concerning the acquisition programs in the mission area of interest. In addition, it is desirable to conduct excursions such as different assumptions about the DoD Component's top-line projected beyond the six-year programming growth.

In preparing affordability assessments, one possible source of data for resource analysts to consider is the Future Years Defense Program (FYDP). The FYDP is an OSD resource database with future projections of resources (funding, manpower, and forces) over the programming period by program, where each program is associated with one (or a few) FYDP entities known as program elements. For acquisition programs, there are usually separate program elements for development and procurement. The FYDP also has comparable historical data going back several years. The FYDP data structure also provides options for assigning FYDP program elements to mission areas. One common approach for assigning resources to mission areas is the use of Defense Mission Categories. Further information on the FYDP, as well as Defense Mission Categories, can be found at the FYDP Structure Management System web site. (Note: Access requires a SIPRNet account.) For projections beyond the FYDP programming period, many DoD Components (or their major commands) have long-range modernization roadmaps which can be incorporated in the assessment. In addition, annual funding projections beyond the FYDP for major defense acquisition programs can be obtained from the appropriate Selected Acquisition Reports.

3.2.3. Full Funding

It has been a long-standing DoD policy to seek full funding of acquisition programs, based on the most likely cost, in the budget year and out-year program years. Experience has shown that full funding is a necessary condition for program stability. DoD Directive 5000.01 affirms this full funding policy. Moreover, DoD Instruction 5000.02 requires full funding-defined as

inclusion of the dollars and manpower needed for all current and future efforts to carry out the acquisition strategy in the budget and out-year program-as part of the entrance criteria for the transition into engineering and manufacturing development.

Full funding and program stability is especially important in joint and international acquisition programs. Underfunding or program instability on the part of one DoD Component can lead to unintended cost growth or instability for another DoD Component in a joint program, or even for another nation in an approved international cooperative program commitment. DoD Instruction 5000.02, Enclosure 10, sections 4 and 5.c impose very strict approval requirements that must be met before DoD Components are permitted to terminate or make significant reduction to their share of approved joint or international programs. DoD Components contemplating termination of an international program should be aware of the termination provisions in the international agreement for that program. Current practice requires the nation terminating its participation in the program to pay substantial termination costs. Therefore, any DoD Component considering unilateral withdrawal from an international agreement must take into account the resultant costs that would be incurred.

For Major Defense Acquisition Programs at Milestone B, the Milestone Decision Authority (MDA) must certify in writing to the Congress that the program is fully funded through the period covered by the Future Years Defense Program (FYDP), relative to reasonable cost and schedule estimates that meet Director, Cost Assessment and Program Evaluation (DCAPE) concurrence. Other certification requirements are listed under 10 U.S.C. 2366b. For all acquisition programs, the MDA normally assesses full funding at all major decision points. As part of this assessment, the MDA reviews the actual funding (in the most recent Future Years Defense Program position) in comparison to the (time-phased) DoD Component Cost Estimate (see section 3.4.2). In addition, the MDA considers the funding recommendations made by DCAPE (for Acquisition Category ID and IAM programs), or the DoD Component Cost Analysis team (for Acquisition Category IC and IAC programs). If the MDA concludes that the current funding does not support the acquisition program, then the acquisition decision memorandum may direct a funding adjustment and/or program restructure in the next FYDP update.

3.2.4. Cost As an Independent Variable

As stated in DoD Directive 5000.01, all participants in the acquisition system are expected to recognize the reality of fiscal constraints, and to view cost as an independent variable. Cost in this context refers to Life-Cycle Cost (see section 3.1.2), which should be treated as equally important as performance and schedule in program decisions. To institutionalize this principle, program managers should consider developing a formal Cost As an Independent Variable (CAIV) plan as part of the acquisition strategy. This section describes one possible approach for developing such a plan.

The implementation steps in a CAIV plan will depend on the type of system and its current phase in the defense acquisition management system. In general, however, a CAIV plan would include the following elements:

Set Cost Goals. The CAIV plan would include cost goals for unit procurement cost and operating and support (O&S) costs. The unit procurement cost goal typically would be established for a specified quantity of systems and a specified peak production rate. The O&S cost goal would be an annual cost per typical deployable unit (e.g., battalion or squadron) or individual system (e.g., ship or missile), given specified and documented ground rules and assumptions (such as the program basing plan and the system operating tempo). The goals should be challenging but realistically achievable. The goals in the CAIV plan might be the same as the cost goals in the Acquisition Program Baseline (APB), or possibly might be more aggressive. Conceivably, the APB goals might be more conservative for programs with a greater degree of risk, to provide some margin of error.

Perform Trade-off Studies. Cost, schedule, and performance may be traded off within the "trade space" between thresholds and objectives documented in the capability needs document. The CAIV plan would show the timing, content, and approach for the specific trade studies to be performed. Over time, as the system design matures, the trade studies become more refined and specialized. Note that DoD Instruction 5000.02, Enclosure 7, paragraph 6 requires that the fully burdened cost of delivered energy shall be used in trade off analyses conducted for all DoD tactical systems with end items that create a demand for energy.

Establish Cost Performance Integrated Product Team. Although led by the program manager, the CAIV process requires collaboration with the user as well as other acquisition and logistics organizations. The CAIV plan would designate a Cost Performance Integrated Product Team (IPT), which most likely would receive considerable support from the system contractor. The Cost Performance IPT would monitor the CAIV implementation and oversee the trade studies.

Provide Incentives. The elements of the acquisition strategy should describe incentives to the contractor that directly support, or are at least complementary to, the CAIV plan. Such incentives might include award fees, sharing of cost savings, or other (positive or negative) incentives. Chapter 2 provides further discussion on contract incentives.

Establish Metrics. The CAIV plan should address how metrics will be established to track progress and achievement of unit procurement and O&S cost goals. The plan should identify how progress toward achieving the goals will be monitored and reported. The plan also should describe how cost estimates will be updated and refined over time, and compared to the original cost goals. The plan should identify specific organizational responsibilities, and identify related major events where progress toward achieving goals will be assessed.

As part of the Reduction of Total Ownership Costs (R-TOC) Program, the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics/Systems and Software

Engineering has developed a template that could be used as a guideline in the development of a CAIV implementation plans. The use of this template is optional. The template may be found at the DoD R-TOC web site. This web site is restricted to .mil users; the template is designated as "For Official Use Only."

3.3. Analysis of Alternatives

3.3.1. Introduction

The Analysis of Alternatives (AoA) is an important element of the defense acquisition process. An AoA is an analytical comparison of the operational effectiveness, suitability, and life-cycle

cost (or total ownership cost, if applicable) of alternatives that satisfy established capability needs. Initially, after the Materiel Development Decision, the AoA is initiated to examine potential materiel solutions with the goal of identifying the most promising option, thereby guiding the Materiel Solution Analysis phase (see section 3.3.2). Subsequently, an update to the AoA is initiated at the start of the Technology Development Phase and is reviewed at Milestone B (which usually represents the first major funding commitment to the acquisition program). The update to the AoA is used to refine the proposed materiel solution, as well as reaffirm the rationale, in terms of cost-effectiveness, for initiation of the program into the formal systems acquisition process. For Major Defense Acquisition Programs at Milestone A, the Milestone Decision Authority (MDA) must certify in writing to the Congress that the Department has completed an AoA consistent with study guidance developed by the Director of Cost Assessment and Program Evaluation (DCAPE), in addition to meeting other certification criteria (10 U.S.C. 2366a). For Major Defense Acquisition Programs at Milestone B, the Milestone Decision Authority (MDA) must certify in writing to the Congress that the Department has completed an AoA with respect to the program in addition to meeting other certification criteria (10 U.S.C. 2366b). An AoA normally is not required at Milestone C unless significant changes to threats, costs, or technology have occurred, or the analysis is otherwise deemed necessary by the MDA.

In practice, AoA issues vary somewhat between AoAs for weapon and other tactical systems, and AoAs for major automated information systems. Sections 3.3.2, 3.3.3, and 3.3.4 provide discussion about AoAs that may be of general interest, although much of the discussion is focused on weapon systems. Section 3.3.5 discusses the AoA process for major automated information systems.

3.3.2. Role of the Analysis of Alternatives (AoA) as Part of the Materiel Solution Analysis

The analysis of alternatives process is expected to play a key role in support of the Materiel Solution Analysis Phase. After a program has an approved Materiel Development Decision, the analysis of alternatives process is expected to contribute to the selection of a preferred materiel solution that satisfies the capability need documented in the approved Initial Capabilities Document (ICD). The role of this analytic support is shown graphically in Figure 3.3.2.F1.

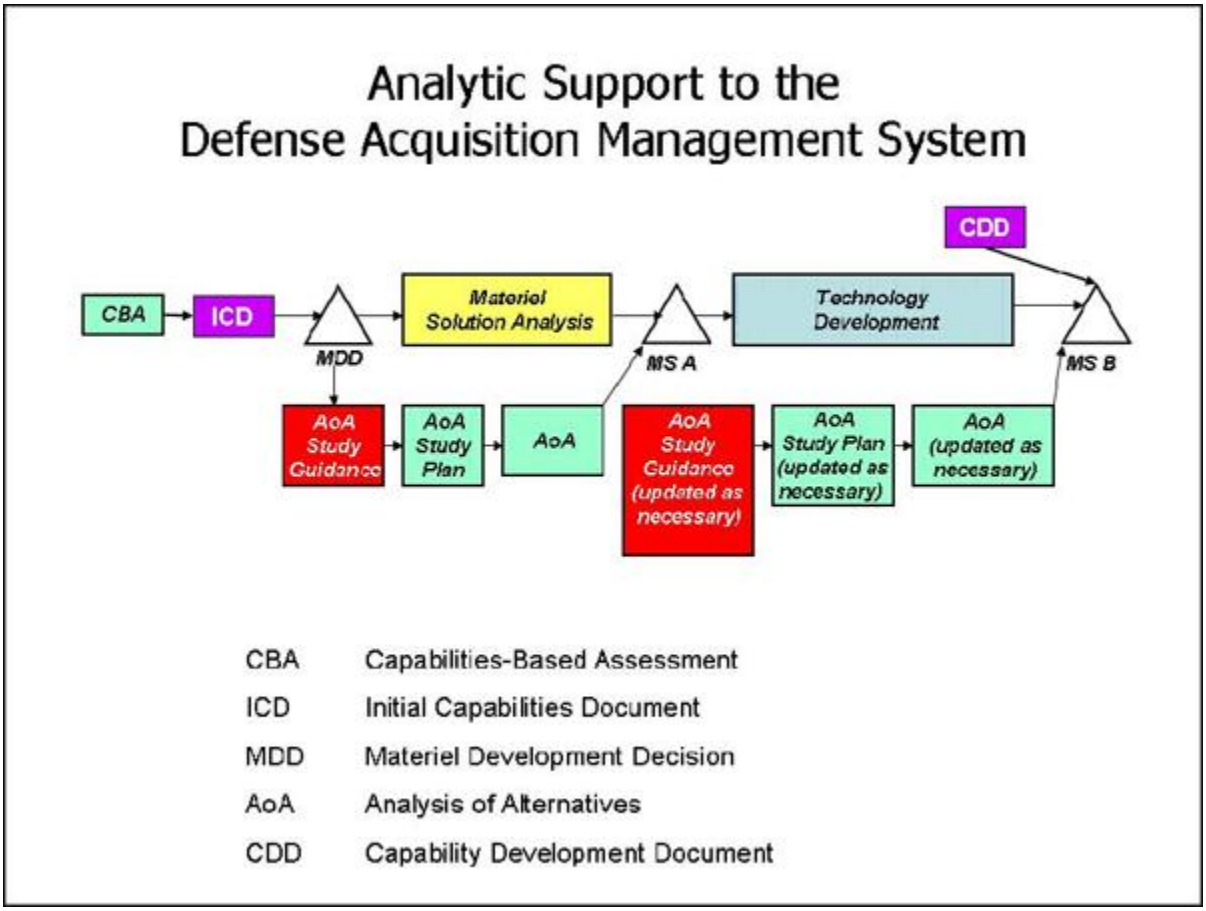


Figure 3.3.2.F1. Analytic Support to the Defense Acquisition Management System

The Director, Cost Assessment and Program Evaluation (DCAPE) develops and approves study guidance for the AoA. The guidance is developed with the input of other DoD officials, and DCAPE provides the approved guidance at the MDD review. Following a successful MDD review, the MDA directs initiation of the AoA in the acquisition decision memorandum (ADM) and includes the AoA study guidance as an attachment to the ADM. Following receipt of the AoA study guidance, the lead DoD Component prepares an AoA study plan that describes the intended methodology for the management and execution of the AoA. A suggested template for the AoA study plan is provided in section 3.3.3. The study plan is coordinated with the MDA, and approved by the DCAPE, prior to the start of the AoA.

The study guidance shall require, at minimum, full consideration of possible trade-offs among cost, schedule, and performance objectives for each alternative considered. The study guidance shall also require an assessment of whether or not the joint military requirement can be met in a manner that is consistent with the cost and schedule objectives recommended by the JROC.

The AoA study guidance and resulting AoA plan should build upon the prior analyses conducted as part of the Joint Capabilities Integration and Development System (JCIDS). The JCIDS

process is briefly described in section 1.3, and is fully described in CJCS Instruction 3170.01. The JCIDS analysis process that leads to an approved Initial Capabilities Document (ICD) is built upon the analysis known as the Capabilities-Based Assessment (CBA). The CBA provides recommendations (documented in the ICD) to pursue a materiel solution to an identified capability gap that meets an established capability need. The CBA does not provide specific recommendations as to a particular materiel solution, but rather provides a more general recommendation as to the type of materiel solution (such as Information Technology system, incremental improvement to an existing capability, or an entirely new "breakout" or other transformational capability). In this way, the ICD can be used to establish boundary conditions for the scope of alternatives to be considered in the subsequent AoA. The AoA study guidance should be crafted to provide a fair balance between focusing the AoA and ensuring that the AoA considers a robust set of novel and imaginative alternatives.

The final AoA supporting a Milestone A decision is provided to the DCAPE not later than 60 days prior to the milestone decision review meeting. The evaluation criteria to be addressed in this assessment are provided in DoD Instruction 5000.02, Enclosure 7, paragraph 5, and are discussed further in section 3.3.4.1.

3.3.2.1. Role of the Analysis of Alternatives (AoA) in Evolutionary Acquisition

The AoA is used to identify the most promising end-state materiel solution, but the AoA also can play a supporting role in crafting a cost-effective and balanced evolutionary acquisition strategy. The alternatives considered in the AoA may include alternative evolutionary paths, each path consisting of intermediate nodes leading to the proposed end-state solution. In this way, the Materiel Solution Analysis can help determine the best path to the end-state solution, based on a balanced assessment of technology maturity and risk, and cost, performance, and schedule considerations (as shown in Figure 3.3.2.1.F1). The rationale for the proposed evolutionary acquisition strategy would be documented as part of the Technology Development Strategy.

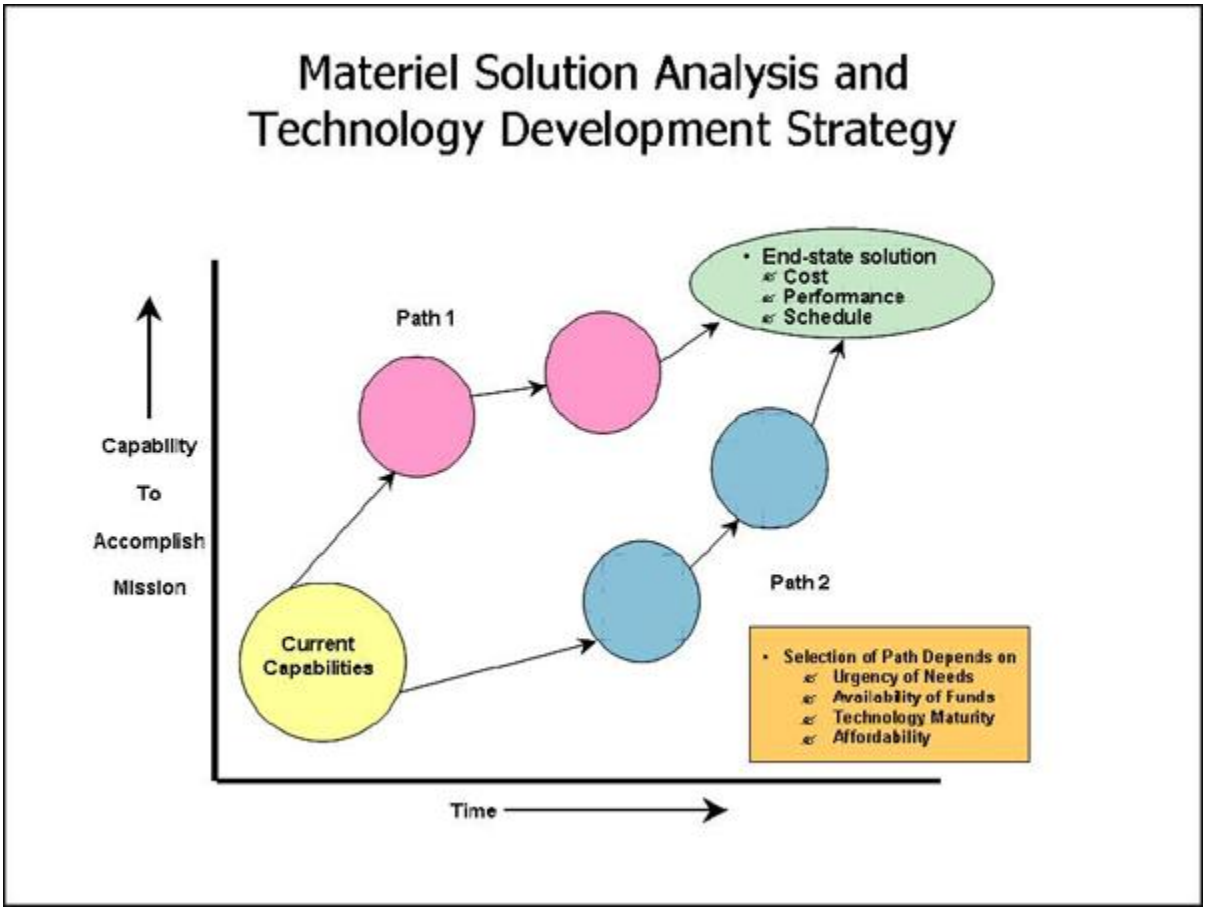


Figure 3.3.2.1.F1. Establishment of an Evolutionary Acquisition Strategy

3.3.3. Analysis of Alternatives (AoA) Study Plan

The first major step leading to a successful AoA is the creation and coordination of a well-considered analysis plan. The study plan should establish a roadmap of how the analysis will proceed, and who is responsible for doing what. At minimum, the study plan should facilitate full consideration of possible trade-offs among cost, schedule, and performance objectives for each alternative considered, as well as an assessment of whether or not the joint military requirement can be met in a manner that is consistent with the cost and schedule objectives recommended by the JROC.

A recommended outline for the AoA plan would resemble the following:

- Introduction
  - Background
  - Purpose
  - Scope

- Ground Rules
  - Scenarios
  - Threats
  - Environment
  - Constraints and Assumptions
  - Timeframe
  - Excursions
- Alternatives
  - Description of Alternatives
  - Nonviable Alternatives
  - Operations Concepts
  - Sustainment Concepts
- Determination of Effectiveness Measures
  - Mission Tasks
  - Measures of Effectiveness
  - Measures of Performance
- Effectiveness Analysis
  - Effectiveness Methodology
  - Models, Simulations, and Data
  - Effectiveness Sensitivity Analysis
- Cost Analysis
  - Life-Cycle Cost Methodology
  - Additional Total Ownership Cost Considerations (if applicable)
  - Fully Burdened Cost of Delivered Energy (if applicable)
  - Models and Data
  - Cost Sensitivity and/or Risk Analysis
- Cost-Effectiveness Comparisons
  - Cost-Effectiveness Methodology
  - Displays or Presentation Formats
  - Criteria for Screening Alternatives
- Organization and Management
  - Study Team/Organization
  - AoA Review Process
  - Schedule

Of course, every AoA is unique, and the above outline may need to be tailored or streamlined to support a given situation. Each point in the above outline is discussed further in the next several sections.

3.3.3.1. Analysis of Alternatives (AoA) Study Plan-Introduction

The introduction to the AoA plan describes the developments that led to the AoA, including prior relevant analyses (such as the Capabilities-Based Assessment. It should reference the applicable capability needs document(s) and other pertinent documents, and highlight the capability gaps

being addressed through the applicable capability needs. The introduction should describe the applicable AoA study guidance and any other terms of reference. It also should provide a broad overview of the planned AoA that describes in general terms the level of detail of the study, and the scope (breadth and depth) of the analysis necessary to support the specific milestone decision.

3.3.3.2. Analysis of Alternatives (AoA) Study Plan-Ground Rules

The ground rules described in the analysis plan include the scenarios and threats, as well as the assumed physical environment and any constraints or additional assumptions. The scenarios are typically derived from defense planning scenarios and associated joint operational plans, augmented by more detailed intelligence products such as target information and enemy and friendly orders of battle. Environmental factors that impact operations (e.g., climate, weather, or terrain) are important as well. In addition, environment, safety, and occupational health factors associated with the use of chemical and/or biological weapons may need to be considered as excursions to the baseline scenario(s).

The study plan should describe what future timeframe, or timeframes, will be considered in the analysis. Often, the time period(s) selected will be determined by the time period(s) assumed in the DoD-approved planning scenario. However, there is some flexibility on this point, especially if something significant-such as the deployment of a new capability, or the retirement of a legacy system-is projected to occur one or two years after one of the time periods in the scenario. A common and desirable practice is to consider two time periods of interest, say "near-term" and "far-term," separated by a decade or so.

The AoA study plan should describe the planned analytic excursions to the baseline scenarios and other major ground rules. Such excursions are strongly encouraged in order to explore any impact of changing threat levels, warning times, involvement of allied forces, political constraints on basing or overflights, just to name a few issues. These excursions can be used to see if there any major issues that are critical to the relative cost-effectiveness of the alternatives considered in the AoA.

3.3.3.3. Analysis of Alternatives (AoA) Study Plan-Range of Alternatives

The analysis plan also should document the range of alternatives to be addressed in the analysis. In many cases, there will be a minimum set of alternatives required by the initial analysis guidance. Additional direction during subsequent AoA reviews may insert yet other alternatives. Practically, the range of alternatives should be kept manageable. Selecting too few or too many are both possibilities, but experience has shown that selecting too many, exceeding the available resources of the AoA study team, is the greater concern. The number of alternatives can be controlled by avoiding similar but slightly different alternatives and by early elimination of alternatives (due to factors such as unacceptable life-cycle cost or inability to meet Key Performance Parameters). In many studies, the first alternative (base case) is to retain one or more existing systems, representing a benchmark of current capabilities. An additional

alternative based on major upgrades and/or service-life extensions to existing systems also may be considered.

For each alternative, evaluating its effectiveness and estimating its life-cycle cost (or total ownership cost, if applicable) requires a significant level of understanding of its operations and support concepts. The operations concept describes the details of the peacetime, contingency, and wartime employment of the alternative within projected military units or organizations. It also may be necessary to describe the planned basing and deployment concepts (contingency and wartime) for each alternative. The sustainment concept for each alternative describes the plans and resources for system training, maintenance, and other logistics support.

It is important that the alternatives considered in the AoA should address alternative concepts for maintenance, training, supply chain management, and other major sustainment elements. In this way, the AoA can identify the preferred materiel solution not only in terms of traditional performance and design criteria (e.g., speed, range, lethality), but also in terms of support strategy and sustainment performance as well. In other words, the AoA should describe and include the results of the supportability analyses and trade-offs conducted to determine the most cost-effective support concept as part of the proposed system concept. Further information on the role of the AoA concerning system support issues is provided in section 5.4.1.2.1.

3.3.3.4. Analysis of Alternatives (AoA) Study Plan-Effectiveness Measures

The analysis plan should describe how the AoA will establish metrics associated with the military worth of each alternative. Military worth often is portrayed in AoAs as a hierarchy of mission tasks, measures of effectiveness, and measures of performance. Military worth is fundamentally the ability to perform mission tasks, which are derived from the identified capability needs. Mission tasks are usually expressed in terms of general tasks to be performed to correct the gaps in needed capabilities (e.g., hold targets at risk, or communicate in a jamming environment). Mission tasks should not be stated in solution-specific language. Measures of effectiveness are more refined and they provide the details that allow the proficiency of each alternative in performing the mission tasks to be quantified. Each mission task should have at least one measure of effectiveness supporting it, and each measure of effectiveness should support at least one mission task. A measure of performance typically is a quantitative measure of a system characteristic (e.g., range, weapon load-out, logistics footprint, etc.) chosen to enable calculation of one or more measures of effectiveness. Measures of performance are often linked to Key Performance Parameters or other parameters contained in the approved capability needs document(s). Also, measures of performance are usually the measures most directly related to test and evaluation criteria.

3.3.3.5. Analysis of Alternatives (AoA) Study Plan-Effectiveness Analysis

The analysis plan spells out the analytic approach to the effectiveness analysis, which is built upon the hierarchy of military worth, the assumed scenarios and threats, and the nature of the selected alternatives. The analytic approach describes the level of detail at various points of the

effectiveness analysis. In many AoAs involving combat operations, the levels of effectiveness analysis can be characterized by the numbers and types of alternative and threat elements being modeled. A typical classification would consist of four levels: (1) system performance, based on analyses of individual components of each alternative or threat system, (2) engagement, based on analyses of the interaction of a single alternative and a single threat system, and possibly the interactions of a few alternative systems with a few threat systems, (3) mission, based on assessments of how well alternative systems perform military missions in the context of many-on-many engagements, and (4) campaign, based on how well alternative systems contribute to the overall military campaign, often in a joint context. For AoAs involving combat support operations, the characterization would need to be modified to the nature of the support.

Nevertheless, most AoAs involve analyses at different levels of detail, where the outputs of the more specialized analysis are used as inputs to more aggregate analyses. At each level, establishing the effectiveness methodology often involves the identification of suitable models (simulation or otherwise), other analytic techniques, and data. This identification primarily should be based on the earlier selection of measures of effectiveness. The modeling effort should be focused on the computation of the specific measures of effectiveness established for the purpose of the particular study. Models are seldom good or bad per se; rather, models are either suitable or not suitable for a particular purpose.

It also is important to address excursions and other sensitivity analyses in the overall effectiveness analysis. Typically, there are a few critical assumptions that often drive the results of the analysis, and it is important to understand and point out how variations in these assumptions affect the results. As one example, in many cases the assumed performance of a future system is based on engineering estimates that have not been tested or validated. In such cases, the effectiveness analysis should describe how sensitive the mission or campaign outcomes are to the assumed performance estimates.

3.3.3.6. Analysis of Alternatives (AoA) Study Plan-Cost Analysis

The AoA plan also describes the approach to the life-cycle cost (or total ownership cost (see section 3.1.5, if applicable) analysis. The cost analysis normally is performed in parallel with the operational effectiveness analysis. It is equal in importance as part of the overall AoA process. It estimates the total life-cycle cost (or total ownership cost) of each alternative, and its results are later combined with the operational effectiveness analysis to portray cost-effectiveness comparisons. What is important to emphasize is that the cost analysis will be a major effort that will demand the attention of experienced, professional cost analysts.

The principles of economic analysis apply to the cost analysis in an AoA. Although the cost estimates used in an AoA originally are estimated in constant dollars, they should be adjusted for discounting (time value of money), accounting for the distribution of the costs over the study time period of interest. In addition, the cost estimates should account for any residual values associated with capital assets that have remaining useful value at the end of the period of

analysis. Further guidance on economic analysis is provided in DoD Instruction 7041.3, "Economic Analysis for Decisionmaking."

The cost analysis should also describe the planned approach for addressing the Fully Burdened Cost of Energy, for those AoAs where this issue is applicable. See section 3.3.4.1 for further information on this topic.

Further information on the recommended analytic approach for cost estimates is provided in section 3.7.

3.3.3.7. Analysis of Alternatives (AoA) Study Plan-Cost-Effectiveness Comparisons

Typically, the next analytical section of the AoA plan deals with the planned approach for the cost-effectiveness comparisons of the study alternatives. In most AoAs, these comparisons involve alternatives that have both different effectiveness and cost, which leads to the question of how to judge when additional effectiveness is worth additional cost. Cost-effectiveness comparisons in theory would be best if the analysis structured the alternatives so that all the alternatives have equal effectiveness (the best alternative is the one with lowest cost) or equal cost (the best alternative is the one with greatest effectiveness). Either case would be preferred; however, in actual practice, in many cases the ideal of equal effectiveness or equal cost alternatives is difficult or impossible to achieve due to the complexity of AoA issues. A common method for dealing with such situations is to provide a scatter plot of effectiveness versus cost. Figure 3.3.3.7.F1 presents a notional example of such a plot.

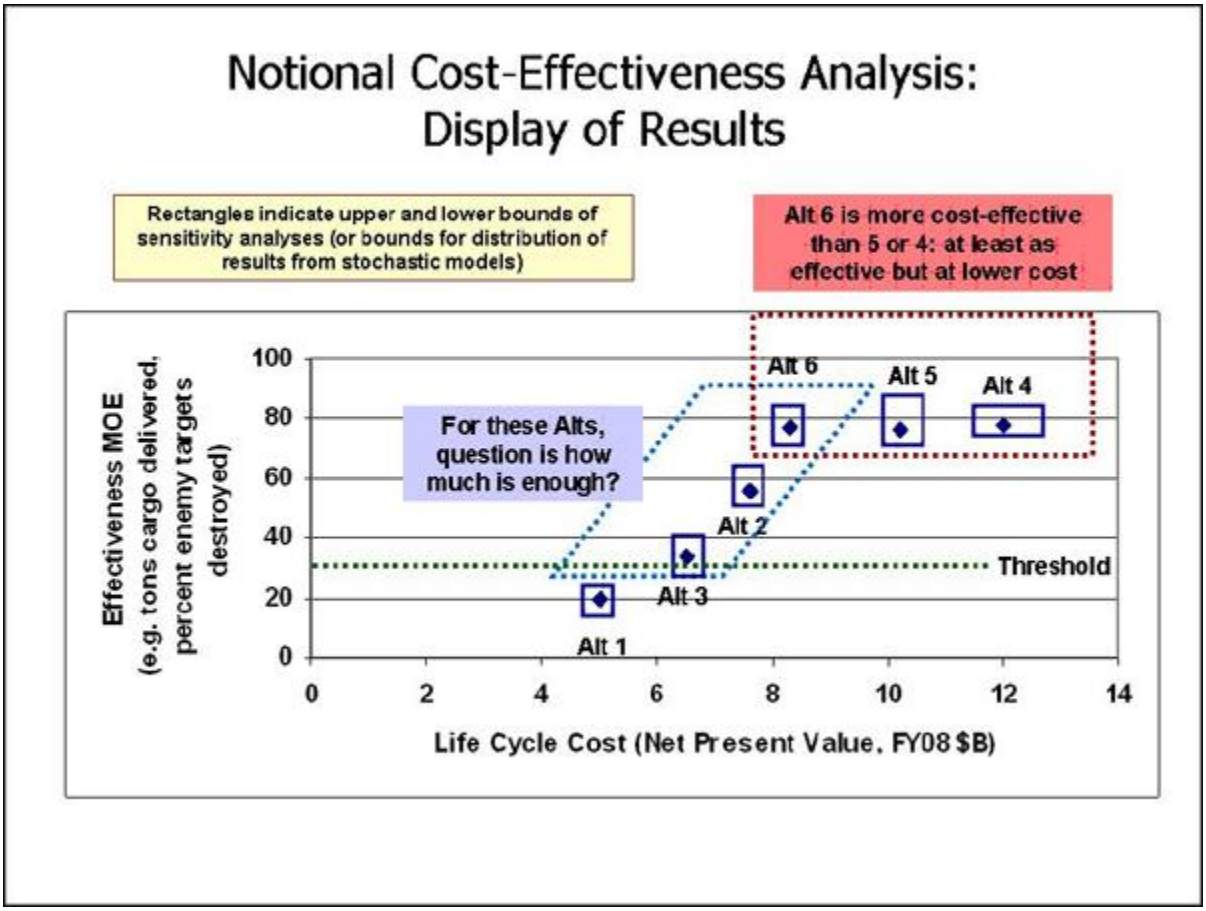


Figure 3.3.3.7.F1. Sample Scatter Plot of Effectiveness versus Cost

Note that the notional sample display shown in Figure 3.3.3.7.F1 does not make use of ratios (of effectiveness to cost) for comparing alternatives. Usually, ratios are regarded as potentially misleading because they mask important information. The advantage to the approach in the figure above is that it reduces the original set of alternatives to a small set of viable alternatives for decision makers to consider.

3.3.3.8. Analysis of Alternatives (AoA) Study Plan-Organization and Management

Finally, the AoA plan should address the AoA study organization and management. Often, the AoA is conducted by a working group (study team) led by a study director and staffed appropriately with a diverse mix of military, civilian, and contractor personnel. Program offices or similar organizations may provide assistance or data to the AoA study team, but (per DoD Instruction 5000.02, Enclosure 7) the responsibility for the AoA may not be assigned to a program manager, and the study team members should not reside in a program office. In some

cases, the AoA may be assigned to an in-house analytic organization, a federally funded research and development center, or some other similar organization.

The AoA study team is usually organized along functional lines into panels, with a chair for each panel. Typical functional areas for the panels could be threats and scenarios, technology and alternatives (responsible for defining the alternatives), operations and support concepts (for each alternative), effectiveness analysis, and cost analysis. In many cases, the effectiveness panel occupies the central position and integrates the work of the other panels. The study plan also should describe the planned oversight and review process for the AoA. It is important to obtain guidance and direction from senior reviewers with a variety of perspectives (operational, technical, and cost) throughout the entire AoA process.

The analysis plan is fundamentally important because it defines what will be accomplished, and how and when it will be accomplished. However, the plan should be treated as a living document, and updated as needed throughout the AoA to reflect new information and changing study direction. New directions are inevitably part of the AoA process, and so the analysis should be structured so as to be flexible. Frequently, AoAs turn out to be more difficult than originally envisioned, and the collaborative analytical process associated with AoAs is inherently slow. There are often delays in obtaining proper input data, and there may be disagreements between the study participants concerning ground rules or alternatives that lead to an increase in excursions or cases to be considered. Experience has shown that delays for analyses dealing with Special Access materials can be especially problematic, due to issues of clearances, access to data, storage, modeling, etc. It is often common for the study director to scale back the planned analysis (or at least consider doing so) to maintain the study schedule.

3.3.4. Analysis of Alternatives Final Results

3.3.4.1. Analysis of Alternatives (AoA) Final Results and Assessment

Normally, the final results of the AoA initially are presented as a series of briefings. For potential and designated major defense acquisition programs (Acquisition Category (ACAT) I) and major automated information systems (ACAT IA), the final AoA results are provided to the Office of the Director, Cost Assessment and Program Evaluation (CAPE), no later than 60 days prior to the milestone decision meeting (Defense Acquisition Board or Information Technology Acquisition Board review). Providing emerging results to CAPE prior to the final briefing is wise to ensure that there are no unexpected problems or issues. For other programs, the AoA results should be provided to the DoD Component entity equivalent to CAPE, if applicable. In any case, the AoA final results should follow all of the important aspects of the study plan, and support the AoA findings with the presentation. In particular, all of the stated AoA conclusions and findings should follow logically from the supporting analysis.

Having received the final AoA briefing(s), the CAPE evaluates the AoA and provides an independent assessment to the Head of the DoD Component (or the Principal Staff Assistant) and to the Milestone Decision Authority. DoD Instruction 5000.02, Enclosure 7, provides the

evaluation criteria for this assessment. According to the Instruction, the CAPE, in collaboration with the OSD and Joint Staff, shall assess the extent to which the AoA:

1. Illuminated capability advantages and disadvantages;
2. Considered joint operational plans;
3. Examined sufficient feasible alternatives;
4. Discussed key assumptions and variables and sensitivity to changes in these;
5. Calculated costs; and,
6. Assessed the following:
    - Technology risk and maturity;
    - Alternative ways to improve the energy efficiency of DoD tactical systems with end items that create a demand for energy, consistent with mission requirements and cost effectiveness; and
    - Appropriate system training to ensure that effective and efficient training is provided with the system.

The recommended template for the AoA study plan provided in section 3.3.3 provides considerable guidance for conducting an AoA that would be responsive to the first five assessment criteria.

For the issue of technology risk and maturity, section 3.3.2.1 provides a suggested approach where the AoA can help craft a cost-effective evolutionary acquisition strategy that is based on a balanced assessment of technology maturity and risk, as well as cost, performance, and schedule considerations.

For the issue of energy efficiency (applicable to tactical systems with end items that create a demand for delivered fuel or other forms of energy), section 3.1.6 describes the analytic construct known as the Fully Burdened Cost of Delivered Energy; the Department now intends for this construct to play a major role in applicable AoAs.

For the issue of system training, the AoA should consider alternatives that provide for the individual, collective, and joint training for system operators, maintainers, and support personnel. The training system includes simulators and other training equipment, as well as supporting material such as computer-based interactive courseware or interactive electronic technical manuals. Where possible, the alternatives should consider options to exploit the use of new learning techniques, simulation technology, embedded training (i.e., training capabilities built into, strapped onto, or plugged into operational systems) and/or distributed learning to promote the goals of enhancing user capabilities, maintaining skill proficiencies, and reducing individual and collective training costs. Further information on system training is provided in section 6.3.3.

In addition to addressing the assessment criteria explicitly identified in DoD Instruction 5000.02, Enclosure 7, the AoA should also address alternative concepts for maintenance, supply chain management, and other sustainment elements (see Chapter 5 of this Guidebook).

3.3.4.2. Analysis of Alternatives (AoA) Final Report

Usually, in addition to a final briefing, the AoA process and results are documented in a written final report. The report typically is not published formally by the time of the program milestone decision review, due to schedule constraints. However, the report nevertheless may be important to the historical record of the program, since the report serves as the principal supporting documentation for the AoA. The report also may serve as a reference source for analysts conducting future AoAs. The final report can follow the same format as the study plan, with the addition of these sections:

- Effectiveness Analysis
  - Effectiveness Results
- Cost Analysis
  - Life-Cycle Cost (or Total Ownership Cost, if applicable) Results
- Cost-Effectiveness Comparisons
  - Cost-Effectiveness Results
  - Assessment of Preferred Alternative(s)

By following the same format, much of the material from the (updated) study plan can be used in the final report.

3.3.5. Analysis of Alternatives (AoA) Considerations for Major Automated Information Systems (MAIS)

DoD Instruction 5000.02, Enclosure 4, Table 2-1 and Table 3 require an AoA for MAIS programs at milestone decisions. Much of the discussion on AoAs provided in the earlier sections of the Guidebook is more applicable to weapon systems, and needs to be modified somewhat for MAIS programs. This section discusses AoA issues for MAIS programs.

The AoA should include a discussion of whether the proposed program (1) supports a core/priority mission or function performed by the DoD Component, (2) needs to be undertaken because no alternative private sector or governmental source can better support the function, and (3) supports improved work processes that have been simplified or otherwise redesigned to reduce costs, improve effectiveness, and make maximum use of commercial off-the-shelf technology. The analysis should be tied to benchmarking and business process reengineering studies (such as analyses of simplified or streamlined work processes, or outsourcing of non-core functions).

For all MAIS program AoAs, one alternative should be the status quo alternative as used in the Economic Analysis, and one alternative should be associated with the proposed MAIS program. Other possible alternatives could be different system, network, and/or data architectures, or they might involve different options for the purchase and integration of commercial-off-the-shelf products, modifications, and upgrades of existing assets, or major in-house development.

Most likely, the effectiveness analysis in a MAIS program AoA will not involve scenario-based analysis as is common for the weapon system AoAs. The effectiveness analysis for an MAIS program should be tied to the organizational missions, functions, and objectives that are directly supported by the implementation of the system being considered. The results of the AoA should provide insight into how well the various alternatives support the business outcomes that have been identified as the business goals or capabilities sought. In some cases, it may be possible to express the assessment of effectiveness across the alternatives in monetary terms, and so effectiveness could be assessed as benefits in the framework for the Economic Analysis. In other cases, the effectiveness might be related to measurable improvements to business capabilities or better or timelier management information (leading to improved decision-making, where it can be difficult or impossible to quantify the benefits). In these cases, a common approach is to portray effectiveness by the use of one or more surrogate metrics. Examples of such metrics might be report generation timeliness, customer satisfaction, or supplier responsiveness. In addition to management information, the effectiveness analysis also should consider information assurance and interoperability issues.

The cost analysis supporting the AoA should follow the framework of the Economic Analysis. The life-cycle cost estimates of the alternatives considered in the AoA should be consistent with and clearly linked to the alternatives addressed in the Economic Analysis. Both the effectiveness analysis and the cost analysis should address the risks and uncertainties for the alternatives, and present appropriate sensitivity analysis that describes how such uncertainties can influence the cost-effectiveness comparison of the alternatives.

The appropriate sponsor or domain owner should lead the development of the AoA for a MAIS program. Experience has shown that the MAIS programs for which the sponsor or domain owner engages with the Office of the Director, Cost Assessment and Program Evaluation (CAPE) early in the process are much more likely to be successful than those that select a preferred alternative before contacting CAPE or before completing the AoA.

The DoD Component performing the AoA should develop a study plan that addresses the AoA study guidance, as applicable. At a minimum, the study plan should address the following topics:

AoA Study Plan – Outline

a. Introduction (Background, Purpose & Scope)
b. Ground Rules: Constraints and Assumptions
c. Description of Alternatives
d. Determination of Effectiveness Measures
    1. Measures of Effectiveness (MOEs) – operationally relevant & measurable
    2. Measures of Performance – technical characteristics required to satisfy MOEs and are measurable & employed as an operational test criteria
e. Effectiveness Analysis Methodology
f. Cost Analysis
g. Cost-Effectiveness Comparisons

h. Risk & Sensitivity Analysis

    1. Mission
    2. Technology
    3. Programmatic, to include funding

i. Study Organization and Management
j. Schedule, with associated deliverables

3.4. Cost Estimation for Major Defense Acquisition Programs

3.4.4.2.1. Contractor Cost Data Reporting (CCDR)

3.4.4.2.2. Software Resources Data Reporting (SRDR)

3.4.4.3. Visibility and Management of Operating and Support Costs (VAMOSC)

3.4.1. Independent Cost Estimates

Independent cost estimates of the full life-cycle cost for a Major Defense Acquisition Program (Acquisition Category (ACAT) I) are required to be prepared or approved by the Director of Cost Assessment and Program Evaluation (DCAPE) before the approval to proceed with technology development, system development and demonstration (now known as Engineering and Manufacturing Development), and Production and Deployment stages (see 10 U.S.C. 2334(a)(6)(A) and 2434).

The Department's implementation of this requirement is prescribed in DoD Instruction 5000.02, "Operation of the Defense Acquisition System," Table 2-1. For ACAT ID programs, or pre-MDAP projects approaching formal program initiation as a likely ACAT ID program, the responsibility for the independent cost estimate is assigned to OSD Office of Cost Assessment (as described in Section 3.4.3). For the ACAT IC programs, or pre-MDAP projects approaching formal program initiation as a likely ACAT IC program, the responsibility is assigned to the appropriate Service Cost Center or Defense Agency equivalent. The Service Cost Centers are in the financial management organizations of their respective military departments, and are outside of their department's acquisition chain-of-command.

In either case (ACAT ID or ACAT IC), the independent cost estimate is required prior to certification at Milestone A (see 10 U.S.C. 2366a), Milestone B (see 10 U.S.C. 2366b), and before any decision to enter into low-rate initial production or full-rate production. Independent cost estimates are also required in advance of certification following critical cost growth in major defense programs (pursuant to 10 U.S.C. 2433a). In addition, an independent cost estimate may be conducted by the Office of Cost Assessment for an ACAT ID program at any other time as directed by either the DCAPE or the USD(AT&L).

The Congress has required certain risk reporting aspects for MDAP and MAIS programs. For such programs, the Director of Cost Assessment and Program Evaluation (DCAPE) and the Secretary of the Military Department concerned (or the head of the Defense Agency concerned) must state the confidence level used in establishing a cost estimate, the rationale for selecting the confidence level, and, if the confidence level is less than 80 percent, the justification for selecting the lower confidence level.

The confidence level disclosure shall be included in the ADM approving the APB, and in any other cost estimates for MDAP or MAIS programs prepared in association with the estimates prepared in accordance with section 3.4.1, above.

3.4.2. DoD Component Cost Estimates

DoD Instruction 5000.02, "Operation of the Defense Acquisition System," Enclosure 4, Table 3, also directs that a DoD Component Cost Estimate be provided to the Milestone Decision Authority at Milestones A, B, C and the Full-Rate Production Decision Review. These cost estimates must also be provided to the Director, Cost Assessment and Program Evaluation (DCAPE). The generic term "DoD Component Cost Estimate" is used to provide considerable latitude to each military service or defense agency as to the actual responsibility for this cost estimate. In some cases, a military service assigns the responsibility to the program office, which then provides a Program Office Life-Cycle Cost Estimate (PLCCE). In other cases, the DoD Component may adopt a more corporate approach, where an initial program office cost estimate is subject to considerable review and possible adjustment as determined by the Service Cost Center or defense agency equivalent.

In any case, for all Major Defense Acquisition Programs at milestone reviews, it is now anticipated that each DoD Component will establish a DoD Component-level cost position. To support the Department's full funding policy for acquisition programs (see section 3.2.3), as well as specific statutory certifications and regulatory requirements, the DoD Component is expected to fully fund the program to this cost position in the current President's Budget Future Years Defense Program (FYDP), or commit to full funding of the cost position in the next President's Budget FYDP, with identification of specific offsets to address any funding shortfalls that may exist in the current FYDP. In addition, it is expected that the appropriate Deputy Assistant Secretary of the Military Department for Cost and Economics (or defense agency equivalent) will sign for the DoD Component-level cost position, and that the DoD Component Acquisition Executive and the Component Chief Financial Officer will endorse and certify that the FYDP fully funds the program consistent with the DoD Component-level cost position. This policy is promulgated in the OSD Memorandum, "Required Signed and Documented Component-level Cost Position for Milestone Reviews," dated March 12, 2009. This policy will be incorporated into the next update to DoD 5000.4-M, "DoD Cost Analysis Guidance and Procedures."

Although the DoD Component Cost Estimate is required by DoD Instruction 5000.02 at the milestone reviews, it would be considered a good practice for this estimate, or at least its underlying program office cost estimate, to be kept current more frequently, usually on an annual basis. The estimate would be useful in program management and financial management throughout the life of the program. The estimate could be used to support (1) the preparation of annual budget justifications, (2) cost and price analyses associated with contract negotiations or source selection evaluations, (3) the monitoring of progress in achieving program cost goals, and (4) engineering trade-off analyses over the life cycle.

3.4.3. Office of Cost Assessment

The OSD Office of Cost Assessment has been established to provide independent analysis and advice to DoD officials on matters of cost estimation and cost analysis for weapons acquisition programs, including matters of program life-cycle cost. The Director of Cost Assessment and

Program Evaluation (DCAPE) provides policies and procedures for the conduct of all DoD cost estimates and issues guidance relating to the full consideration of life cycle management and sustainability costs. In addition, the DCAPE reviews DoD Component cost estimates and cost analyses conducted in connection with major defense acquisition programs (MDAP) and major automated information systems (MAIS).

The Office of Cost Assessment, under the control and authority of the Director of Cost Assessment and Program Evaluation, is charged with developing, validating, and refining policy, guidance, standards, and methods for the cost community in order to improve management of major defense acquisition and automated information system programs. Per DoDD 5000.04 (to be reissued as DODI 5000.04, Defense Cost Assessment System), some of the Office of Cost Assessment's responsibilities are to:

- Establish substantive guidance on the preparation of life-cycle cost estimates subject to DCAPE review. This guidance in part includes standard definitions of cost terms (see section 3.1) used in the management of DoD acquisition programs. Information on additional Cost Assessment guidance is provided in section 3.4.3.1.
- Sponsor an annual DoD-wide Cost Research Symposium, where representatives from many organizations throughout the DoD Components describe their plans for performing or sponsoring cost research. This symposium facilitates the exchange of cost research, and helps avoid duplication of effort among the DoD Components.
- Establish policy guidance on the Cost and Software Data Reporting (CSDR) system, and monitor its implementation to ensure consistent and appropriate application throughout the DoD. The CSDR system serves as the primary source of acquisition cost data for major defense acquisition programs. The CSDR system is briefly described in section 3.4.4.2, and is fully explained in DoD 5000.04-M-1, "Cost and Software Data Reporting (CSDR) Manual."
- Establish policy guidance on the Visibility and Management of Operating and Support Costs (VAMOSC) Program, and monitor its implementation by each military department. In support of this program, each military department has developed and maintains a collection system for historical operating and support cost data. The VAMOSC program is briefly described in section 3.4.4.3, and formal guidance on the VAMOSC program is contained in DoD 5000.04-M, "DoD Cost Analysis Guidance and Procedures," Section 8.

3.4.3.1. Cost Analysis Reviews (Pre-Milestone Decisions and Full-Rate Production)

3.4.3.1.5. Cost Assessment Review Events-3 Days before OIPT Meeting

The OSD Office of Cost Assessment is a resource for the cost community, designed to facilitate high quality cost estimation and analysis. To accomplish this goal, Cost Assessment will provide early and frequent oversight of programs to ensure that they are able to deliver on cost, schedule, and performance parameters. In order to facilitate review of cost estimates, the Office of Cost Assessment receives the results of all cost estimates and cost analyses and associated studies conducted by the DoD Components for MDAPs and MAIS programs and has timely access to any records and data in the Department.

During the Cost Assessment review process, the Cost Assessment staff may engage in discussion with the DoD Components regarding any discrepancies related to MDAP cost estimates and comment on deficiencies regarding the methodology or execution of cost estimates. Furthermore, Cost Assessment staff are authorized to concur with the choice of a cost estimate used to support the acquisition program baseline (APB).

Although Cost Assessment will provide periodic reviews, the following reviews are regular and required. For programs subject to Cost Assessment review (normally Acquisition Category ID) that are approaching Milestone decisions or the Full-Rate Production Decision Review, the Office of Cost Assessment conducts a comprehensive review and establishes a formal position on a program's life-cycle cost, and advises the Milestone Decision Authority accordingly. The Cost Assessment review consists of the preparation of an independent life-cycle cost estimate, as well as an assessment of the DoD Component Cost Estimate. This section provides a brief summary of the major events associated with the Cost Assessment review, and also provides additional clarifying discussion on the procedures for each event. A more comprehensive description of the Cost Assessment review process is found in DoD 5000.04-M, "DoD Cost Analysis Guidance and Procedures," Section 2.

Table 3.4.3.1.T1 provides a brief summary of the major events and timelines associated with a Cost Assessment review leading to a Defense Acquisition Board milestone decision review:

Event	Date
• Cost Assessment Review Kick-off Meeting ○ Draft Cost Analysis Requirements Description (CARD) Delivered by DoD Component	180 days before Overarching Integrated Product Team (OIPT) meeting
• Cost Assessment Briefs Preliminary Independent Life-Cycle Cost Estimate (LCCE) to Program Manager (PM) ○ Draft Documentation of DoD Component Cost Estimate Delivered by DoD Component	45 days before OIPT meeting

○ Final CARD Delivered by DoD Component	
• Cost Assessment Review Meeting ○ PM Representative Briefs Program Defined in CARD, and Program Office Cost Estimate ○ DoD Component Representative Briefs Component Cost Position, if applicable ○ Cost Assessment Briefs Final Estimate of Independent LCCE to PM	21 days before OIPT meeting
• Final Documentation of DoD Component Cost Estimate Delivered by DoD Component	10 days before OIPT meeting
• OSD Cost Assessment Report Delivered to OIPT Members	3 days before OIPT meeting

Table 3.4.3.1.T1. Cost Assessment Timeline Associated with a DAB Milestone Decision Review

3.4.3.1.1. Cost Assessment Review Events-180 Days before Overarching Integrated Product Team (OIPT) Meeting

The Cost Assessment review process begins roughly six months before the planned Defense Acquisition Board milestone review. At that time, the draft Cost Analysis Requirements Description (CARD) is provided to the Cost Assessment for review. The CARD is used to describe formally the acquisition program for purposes of preparing both the DoD Component Cost Estimate and the Cost Assessment independent cost estimate. The Cost Assessment staff promptly evaluates the CARD for completeness and consistency with other program documents (such as capability needs documents, acquisition strategy, etc.). As part of this evaluation, the Cost Assessment staff may require access to privileged information such as contractor proposals that are proprietary or source selection sensitive. The Cost Assessment staff will follow all necessary procedures to ensure that the integrity of the privileged information is protected, including the signing of any appropriate nondisclosure agreements.

The expectation is that the CARD should be sufficiently comprehensive in program definition to support a life-cycle cost estimate. Normally, the Cost Assessment staff provides any necessary

feedback to the DoD Component if any additional information or revisions are needed. If the CARD is found to be deficient to the point of unacceptability, the Deputy Director, Cost Assessment (DDCA) will advise the OIPT leader that the planned milestone review should be postponed.

At roughly the same time that the draft CARD is submitted, the Cost Assessment staff announces its upcoming review in a formal memo. The memo initiates a working-level kick-off meeting that is held with representatives from the program office cost estimating team, the Cost Assessment independent cost estimate team, and other interested parties (typically DoD Component or OSD staff members). The purpose of the meeting is to discuss requirements and issues for the upcoming milestone review, the scope of the cost estimates, and ground rules and assumptions on which the estimates will be based. Much of the discussion will focus on material provided in the draft CARD. This ensures that both cost teams have a common understanding of the program to be costed. In addition, ground rules are established for Cost Assessment interactions with the program office. The Cost Assessment also coordinates any travel or visit requirements with appropriate DoD Component points of contact.

3.4.3.1.2. Cost Assessment Review Events-45 Days before Overarching Integrated Product Team (OIPT) Meeting

Per DoD Instruction 5000.02, Enclosure 7, section 4, Cost Assessment will brief the preliminary independent Life-Cycle Cost Estimate (LCCE) to the program manager (PM) 45 days before the OIPT meeting. In a similar timeframe, the program office should provide draft documentation of its estimate to the Cost Assessment staff, and, if applicable, the DoD Component should provide draft documentation of the DoD Component Cost Position. The Cost Assessment report eventually submitted to the OIPT and to the Defense Acquisition Board membership provides not only the Cost Assessment independent cost estimate, but also an evaluation of the DoD Component Cost Estimate. It is therefore important for the DoD Components to submit well-documented cost estimates that are ready for review.

The specific standards for the cost documentation are described in DoD 5000.04-M, "DoD Cost Analysis Guidance and Procedures," Sections 1 and 2. In general, the documentation should be sufficiently complete and well organized that a cost professional could replicate the estimate, given the documentation. Along with the draft documentation of the program office cost estimate, the DoD Component provides an updated (and final) Cost Analysis Requirements Description to the Cost Assessment staff. The expectation is that at this point no further changes to program definition will be considered. At the same time that the documents are provided, the Cost Assessment staff will provide feedback and identify any emerging cost issues to the program manager and DoD Component staff, in part based on the Cost Assessment work to date on its independent cost estimate.

3.4.3.1.3. Cost Assessment Review Events-21 Days before Overarching Integrated Product Team (OIPT) Meeting

Per DoD Instruction 5000.02, Enclosure 7, section 4, the Cost Assessment staff will brief the final independent estimate to the program manager 21 days before the OIPT meeting. This is normally handled as part of the Cost Assessment review meeting. At this time, the program office should provide their final estimate to the Cost Assessment staff, and, if applicable, the DoD Component should provide the final DoD Component Cost Position. Other invited OSD and Joint Staff representatives may attend these reviews/exchanges. A typical presentation format for the Cost Assessment review meeting would include:

- Program overview and status
- Program office acquisition cost estimate
    - Summary of results
    - Methodology for high-cost elements
- Rationale for DoD Component cost position, if applicable
- Comparison of (time-phased) program office cost estimate to current funding
- Operating and Support cost estimate

In addition, at the Cost Assessment meeting, the Cost Assessment staff provides any further feedback to the program office and DoD Component staff. If appropriate, the Cost Assessment staff will provide a presentation of the major areas of difference between its independent cost estimate and the program office cost estimate and/or DoD Component cost position.

3.4.3.1.4. Cost Assessment Review Events-10 Days before Overarching Integrated Product Team (OIPT) Meeting

At least 10 days before the OIPT meeting, the DoD Component provides final documentation if its cost estimate (program office cost estimate, or DoD Component Cost Position where applicable).

3.4.3.1.5. Cost Assessment Review Events-3 Days before Overarching Integrated Product Team (OIPT) Meeting

The Cost Assessment staff's final report is delivered to the OIPT leader at least three days before the OIPT meeting. Immediately thereafter, it is distributed to the OIPT members and also is available to the DoD Component staff. The expectation is that any issues had already emerged in prior discussions and that the final Cost Assessment report should not contain any surprises. The report normally is two to three pages, and typically includes the following:

- Summary of DoD Component Cost Estimate
- Summary of Cost Assessment independent cost estimate
- Comparison or reconciliation of the two estimates
- Assessment of program risks
- Comparison of (time-phased) Cost Assessment cost estimate to current program funding
    - Recommendations concerning program funding

3.4.3.2. Cost Estimates for Milestone A Reviews

Per DoD Instruction 5000.02, Enclosure 2, section 5.c.(5), the DoD Component at Milestone A submits a cost estimate for the proposed materiel solution(s). Also, per 10 U.S.C. 2334, the Director of Cost Assessment and Program Evaluation (DCAPE) conducts an independent cost estimate in advance of Milestone A certification. In order to facilitate these estimates, the cost estimating procedures at Milestone A will track those at the other milestone decisions points. This includes the required preparation of a Cost Analysis Requirements Description (CARD, see below), although the early stage of the program development will necessitate less specificity in many of the required elements within the CARD.

The actual process and timing leading to the DoD Component estimate may vary among programs, and therefore a tailored approach should be developed and proposed. Early in the Materiel Solution Analysis Phase, the Program Manager and DoD Component staff should work with the OSD Office of Cost Assessment and Acquisition Resources & Analysis (AT&L/ARA) staffs to develop a plan and schedule for delivery of the cost estimate to support the upcoming Milestone A review. In the near future, the requirement for this plan will be made mandatory and included in the next update to DoD 5000.4-M, "DoD Cost Analysis Guidance and Procedures." At that time, the plan will be subject to approval of the Milestone Decision Authority (MDA).

The DoD Component Cost Estimate, in addition to the DCAPE independent cost estimate, is used to support the MDA certification requirements for Milestone A (10 U.S.C. 2366a and 2334(a)(6)). The emphasis for the Milestone A cost estimate is to provide costing adequate to support the selection of the preferred materiel solution(s) identified by the Analysis of Alternatives, and to support a determination by the MDA that current funding for the Technology Development Phase (required technology development, competitive prototyping, and possibly preliminary design of the end-item system) is adequate. The Milestone A cost estimate is a complete estimate of the system life-cycle cost. However, for the costs associated with the acquisition phases beyond Technology Development (i.e., Engineering and Manufacturing Development, Production and Deployment, and Operations and Support), the Milestone A cost estimate typically would not have the same level of rigor or fidelity as will later cost estimates (prepared for milestones B and beyond). Although the cost estimate addresses the complete life-cycle cost, since it must support the Analysis of Alternatives process, only the program development and procurement costs are subject to certification.

The DoD Component Cost Estimate submitted at Milestone A should be based on a sound description of the program and follow the general requirements of a Cost Analysis Requirements Description (CARD). Understandably, programs at Milestone A are less well-defined than programs at later milestone decision points. The Initial Capabilities Document, Technology Development Strategy, Systems Engineering Plan, Test and Evaluation Strategy, and Analysis of Alternatives, together with the CARD, should be used to provide a technical and programmatic description that should be the foundation for the cost estimate.

To assist in the certification process, the MDA may request that the Cost Assessment staff conduct an independent cost assessment (which is normally a sufficiency review of the DoD Component Cost Estimate). In such cases, the review process and timeline will be established in consultation with the DoD Component on a case-by-case basis. However, the DoD Component normally should plan on providing documentation of its cost estimate to the Cost Assessment staff for review at least 45 days in advance of the Overarching Integrated Product Team meeting. This cost estimate must receive DCAPE approval before Milestone A certification may be granted.

Note that if the certified cost estimate grows at least 25 percent during the Technology Development Phase, then the Program Manager must notify the MDA of the increase. The MDA in turn consults with the Joint Requirements Oversight Council (JROC) to reassess program requirements and the military need(s) for the system. See DoD Instruction 5000.02, Enclosure 2, section 5.c.(3) for further guidance.

3.4.4. Cost Assessment Reporting Requirements

3.4.4.1. Cost Analysis Requirements Description (CARD)

A sound cost estimate is based on a well-defined program. For Acquisition Category (ACAT) I and ACAT IA programs, the CARD is used to formally describe the acquisition program for purposes of preparing both the DoD Component Cost Estimate and the Cost Assessment independent cost estimate. DoD Instruction 5000.02 specifies that for major defense acquisition programs, the CARD will be provided in support of major milestone decision points (Milestone B, Milestone C, or the full-rate production decision review). In addition, for Major Automated Information Systems, the CARD is prepared whenever an Economic Analysis is required. For other acquisition programs, the preparation of a CARD, or an abbreviated CARD-like document with appropriate tailoring, is strongly encouraged to provide a written program description suitable to support a credible life-cycle cost estimate.

The CARD is prepared by the program office and approved by the DoD Component Program Executive Officer. For joint programs, the CARD includes the common program agreed to by all participating DoD Components as well as all unique program requirements of the participating DoD Components. DoD 5000.4-M, "DoD Cost Analysis Guidance and Procedures," Chapter 1, provides further guidelines for CARD content.

3.4.4.1.1. Cost Analysis Requirements Description (CARD) Outline

- System description and characteristics
    - System overview
    - System performance parameters and characteristics
    - Technical and physical description
    - Work breakdown structure

    - Summary of maturity levels of critical technologies
    - Software description and sizing information
    - Interfaces with other systems
    - Subsystem descriptions, as appropriate
- System suitability factors
    - Reliability/Maintainability/Availability
- Predecessor and/or Reference System
- PM's assessment of program risk and risk mitigation measures
- System operational concept
    - Organizational/unit structure
    - Basing and deployment description (peacetime, contingency, and wartime)
- System sustainment concept
    - System logistics concept
        - Maintenance concept
        - Supply management concept
        - Transportation concept
    - Software maintenance concept
    - System training concept
- Time-phased system quantity requirements
- System manpower requirements
- System activity rates (operating tempo or similar information)
- Facilities requirements
- Summary of security or program protection features
- Summary of environment, safety, and occupational health considerations
- System milestone schedule
- Summary of acquisition plan or strategy
- Plans for system disposal
- Track to prior CARD
- Approved or proposed CSDR plan

The above outline will be incorporated into the next update to DoD 5000.4-M, "DoD Cost Analysis Guidance and Procedures," Chapter 1.

3.4.4.1.2. Cost Analysis Requirements Description (CARD) Content

For each topic listed in the suggested outline, the CARD should provide information and data for the program to be costed. In addition, the CARD should include quantitative comparisons between the proposed system and a predecessor and/or reference system for the major topics, as much as possible. A reference system is a currently operational or pre-existing system with a mission similar to that of the proposed system. It is often the system being replaced or augmented by the new acquisition. For a program that is a major upgrade to an existing weapon platform, such as an avionics replacement for an operational aircraft, the new system would be the platform as equipped with the upgrade, and the reference system would be the platform as

equipped prior to the upgrade. For Major Automated Information System programs, the CARD format described above may need to be tailored.

The level of detail provided in the CARD will depend on the maturity of the program. Programs at Milestone B are less well-defined than programs at Milestone C or at full-rate production. In cases where there are gaps or uncertainties in the various program descriptions, these uncertainties should be acknowledged as such in the CARD. This applies to uncertainties in either general program concepts or specific program data. For uncertainties in program concepts, nominal assumptions should be specified for cost-estimating purposes. For example, if the future depot maintenance concept were not yet determined, it would be necessary for the CARD to provide nominal (but specific) assumptions about the maintenance concept. For uncertainties in numerical data, ranges that bound the likely values (such as low, most likely, and high estimates) should be included. In general, values that are "to be determined" (TBD) are not adequate for cost estimating. Dealing with program uncertainty in the CARD greatly facilitates subsequent sensitivity or quantitative risk analyses in the life-cycle cost estimate.

For programs employing an evolutionary acquisition strategy, the CARD should be structured to reflect the specifics of the approach. Although the circumstances may vary somewhat by program, normally the CARD should attempt to include as much of the program, including known future increments, as can be described at the time of the milestone decision review, and clearly document any exclusions for portions of the program that cannot be defined at the present time.

The last section of the CARD should contain a copy of the approved Cost and Software Data Reporting plan (see section 3.4.4.2), if available. If the plan has not yet been approved, then the proposed plan should be included as part of the CARD.

3.4.4.1.3. Cost Analysis Requirements Description (CARD) and Other Program Documentation

Clearly, much of the information needed for the CARD is often available in other program documents. The CARD should stand-alone as a readable document, but can make liberal use of appropriate references to the source documents to minimize redundancy and effort. In such cases, the CARD should briefly summarize the information pertinent to cost in the appropriate section of the CARD, and provide a reference to the source document. DoD Instruction 5000.02, Enclosure 7, paragraph 2, states that the program manager shall synchronize preparation of the CARD with other program documentation, so that the final CARD is consistent with other final program documentation. The source documents should be readily available to the program office and independent cost estimating teams, or alternatively can be provided as an appendix to the CARD. Many program offices provide controlled access to source documents through a web site (perhaps at a ".mil" web address or on the Secret Internet Protocol Router Network).

Common source documents for the CARD include:

- Technology Readiness Assessment (TRA);
- Capability Needs Documents (i.e., Initial Capabilities Document/Capability Development Document/Capability Production Document);
- Acquisition Strategy;
- Life-cycle Sustainment Plan (part of the Acquisition Strategy);
- Test and Evaluation Master Plan;
- Manpower Estimate; and
- Systems Engineering Plan.

In addition, the CARD should be consistent with any contractual solicitations, such as a Request for Proposal or any accompanying document (e.g., System Requirements Document).

3.4.4.1.4. Cost Analysis Requirements Description (CARD) at Milestone B

For programs at Milestone B, DoD Instruction 5000.02, Enclosure 7, paragraph 2, now requires that the program content described in the final CARD reflects the program definition established during the Technology Development Phase. For all MDAPs, the Preliminary Design Review (PDR) may be conducted before the Milestone B approval, and the CARD should also incorporate the results from the PDR for such cases. A nominal timeline for the PDR, final CARD, and completion of the Independent Cost Estimate (ICE) to support the Milestone B review (if the PDR precedes Milestone B approval) is shown in Figure 3.4.4.1.4.F1.

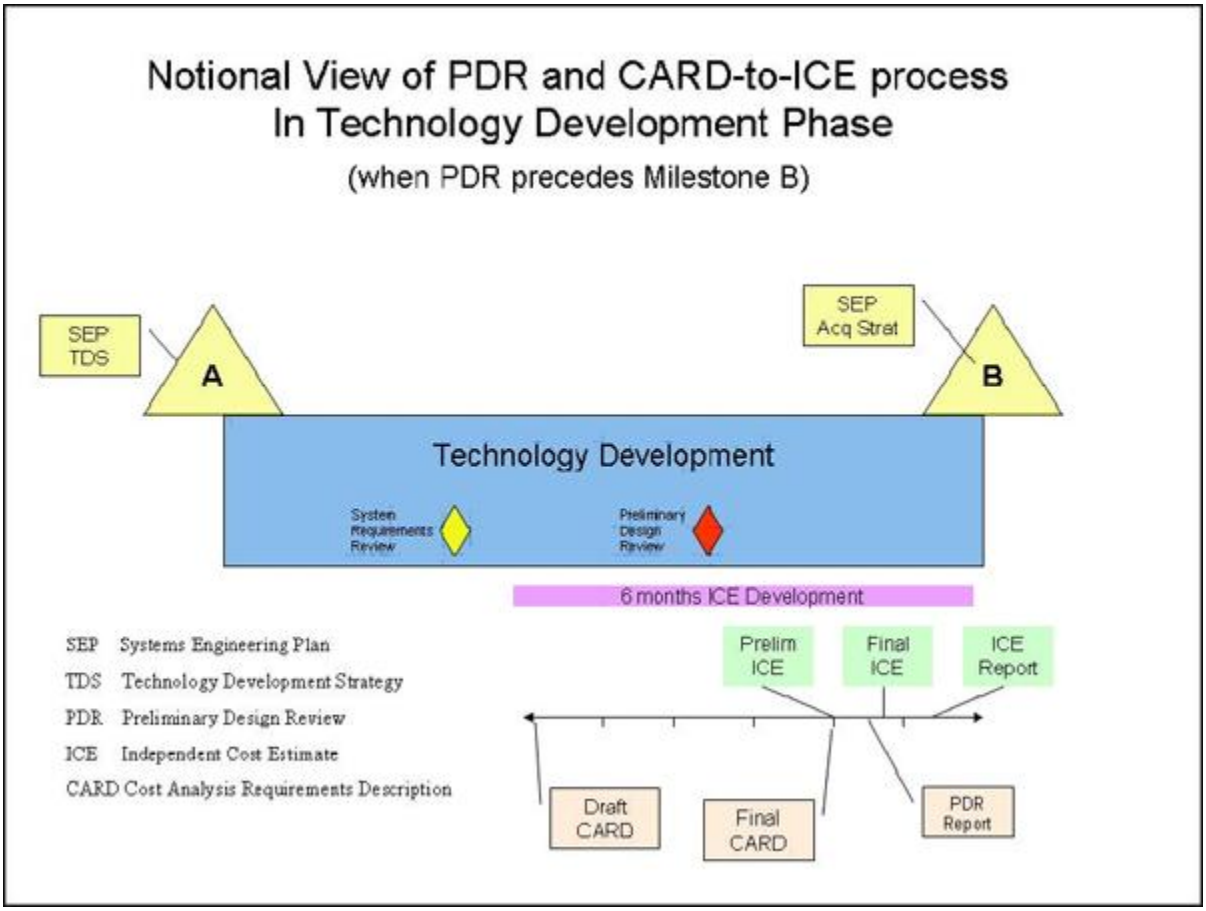


Figure 3.4.4.1.4.F1. Nominal Timeline for Milestone B Review

In this notional example, the results of the PDR are not available by the time of the submission of the draft CARD, and therefore are not reflected in the preliminary ICE. However, the results of the PDR are used to help update the final CARD which in turn is used as the basis for the final ICE.

Another issue for the CARD at the Milestone B review can occur when the Technology Development Phase maintains two or more competing contractor teams (that are producing prototypes of the system) up to and through the PDR. In this situation, there are two possible approaches for the preparation of the CARD. If the competing teams are using similar technologies and designs, then a single generic CARD, based on a nominal Government design, may be used to prepare a single ICE for the nominal design. If the competing teams have significantly different technologies or designs, then it may be necessary to prepare offeror-specific CARDs, which in turn may be used to prepare multiple ICEs. For programs with competing prototype teams approaching a Milestone B review, the DoD Component should discuss its proposed use of a single generic CARD, or use of multiple offeror-specific CARDs, with the Cost Assessment Staff at the Kick-Off Review meeting (see section 3.4.3.1.1), if not earlier.

3.4.4.2. Cost and Software Data Reporting (CSDR)

The CSDR system is the primary means that DoD uses to collect actual cost and related business data on Acquisition Category (ACAT) I and ACAT IA defense contracts. Program managers use the CSDR system to report data on contractor development and production costs and resource usage incurred in performing DoD programs. Its two principal components are contractor cost data reporting (CCDR) and software resources data reporting (SRDR). DoD 5000.04-M-1, "Cost and Software Data Reporting (CSDR) Manual" guides CSDR.

3.4.4.2.1. Contractor Cost Data Reporting (CCDR)

CCDR is the primary means within DoD to systematically collect data on the development and production costs incurred by contractors in performing DoD acquisition program contracts. DoD Instruction 5000.02, Enclosure 4, Table 4, establishes the CCDR requirements for major contracts and sub-contracts (regardless of contract type) associated with Acquisition Category I and IA contracts. The Instruction includes specific CCDR dollar thresholds that can also be found in section 11.3.2.2 of this Guidebook. Detailed procedures and other implementation guidance are found in DoD 5000.04-M-1, "Cost and Software Data Reporting (CSDR) Manual." This manual (as well as downloadable report formats and definitions, specific report examples, and other related information) can be found at the Defense Cost and Resource Center (DCARC) web site. The DCARC is the OSD office responsible for administering the CCDR system. Access to CCDR data is readily provided by the DCARC to DoD government cost analysts, and sponsored support contractors, who are registered users.

3.4.4.2.2. Software Resources Data Reporting (SRDR)

The SRDR system collects software metrics data to supplement the actual Contractor Cost Data Reporting (CCDR) cost data to provide a better understanding and improved estimating of software intensive programs. DoD Instruction 5000.02, Enclosure 4, Table 4, establishes SRDR requirements for major contracts and sub-contracts (regardless of contract type) associated with Acquisition Category I and IA contracts. The Instruction includes specific SRDR dollar thresholds that can also be found in section 11.3.2.2.2 of this Guidebook. Detailed procedures and other implementation guidance are found in DoD 5000.04-M-1, "Cost and Software Data Reporting (CSDR) Manual." Data collected from applicable contracts include type and size of the software application(s), schedule, and labor resources needed for the software development. The CSDR Manual can be found (along with downloadable report formats and definitions, specific report examples, and other related information) at the Defense Cost and Resource Center (DCARC) web site. The DCARC is the OSD office responsible for administering the SRDR system. Access to SRDR data is readily provided by the DCARC to DoD government cost analysts, and sponsored support contractors, who are registered users.

3.4.4.3. Visibility and Management of Operating and Support Costs (VAMOSC)

To achieve visibility into the Operating and Support (O&S) costs of major fielded weapon systems, DoD requires that each military service will maintain an historical data collection system that collects O&S data in a standard presentation format. The Office of Cost Assessment provides policy guidance on this requirement, known as the VAMOSC program, and monitors its implementation by each of the military services. Each service has its own unique VAMOSC data system that tracks actual O&S cost experience for major weapon systems. The data can be displayed by time frame, at various levels of detail, and by functional elements of cost (such as depot maintenance, fuel, consumable items, and so forth). Each VAMOSC system provides not only cost data, but related non-cost data (such as system quantities, operating tempo, or maintenance man-hours) as well. VAMOSC data can be used to analyze trends in O&S cost experience for each major system, as well as to identify and assess major cost drivers. In addition, VAMOSC data are important as a data source for cost estimates of future systems, since cost estimates for future systems are often made by analogy to appropriate predecessor systems. DoD 5000.04-M, "DoD Cost Analysis Guidance and Procedures," Section 8, provides additional direction for VAMOSC.

3.5. Manpower Estimates

For major defense acquisition programs, manpower estimates are required by

- (1) 10 U.S.C. 2434, which directs the Secretary of Defense to consider an estimate of the personnel required to operate, maintain, support, and provide system-related training in advance of approval of the development, or production and deployment; and
- (2) DoD Instruction 5000.02, Enclosure 4, Table 2-1, which directs development of a manpower estimate at Milestones B, C, and full-rate production.

Manpower estimates serve as the authoritative source for out-year projections of active-duty and reserve end-strength, civilian full-time equivalents, and contractor support work-years. As such, references to manpower in other program documentation should be consistent with the manpower estimate once it is finalized. In particular, the manpower estimates should be consistent with the manpower levels assumed in the final Affordability Assessment and the Cost Analysis Requirements Description (CARD).

Organizational responsibilities in preparing the manpower estimate vary by DoD Component. Normally, the manpower estimate is prepared by an analytic organization in the DoD Component manpower community, in consultation with the program manager. The manpower estimates are approved by the DoD Component manpower authority (for the military departments, normally the Assistant Secretary for Manpower and Reserve Affairs).

For Acquisition Category ID programs, a preliminary manpower estimate should be made available at least six months in advance of the Defense Acquisition Board (DAB) milestone review, and should be reflected in the draft CARD due at that time, in order to support the development of cost estimates and affordability assessments. The final manpower estimate should be fully staffed and submitted to the Under Secretary of Defense for Personnel and

Readiness (USD(P&R)) in sufficient time to support the Overarching Integrated Product Team (OIPT) review in preparation of the DAB meeting. Normally this would be four weeks prior to the OIPT review meeting. The USD(P&R) staff will review the final manpower estimate and provide comments to the OIPT.

The exact content of the manpower estimate is tailored to fit the particular program under review. A sample format for the manpower estimate is displayed in the Table 3.5.T1 below. In addition, the estimate should identify if there are any resource shortfalls (i.e., discrepancies between manpower requirements and authorizations) in any fiscal year addressed by the estimate. Where appropriate, the manpower estimate should compare manpower levels for the new system with those required for similar legacy systems, if any. The manpower estimate also should include a narrative that describes the scope of each functional area (operations, maintenance, support, and training), and the methods, factors, and assumptions used to estimate the manpower for each functional area. See section 6.3.1.2 and section 6.3.1.3 for further information concerning manpower.

Table 3.5.T1. Sample Manpower Estimate Format

MANPOWER ESTIMATE
(Program Title)
SERVICE

	FYxx[2]	FYxx+1	FYxx+2	FYxx+3	FYxx+4	...[3]
OPERATE:[4] Military Officers Enlisted Civilian Contractor Sub-Total						
MAINTAIN:[4] Military Officers Enlisted Civilian						

[1]Provide separate estimates for Active and Reserve Components for each Service.
[2]Report manpower by fiscal year (FY) starting with initial fielding and continuing through retirement and disposal of the system (to include environmental clean-up).
[3]Until fielding is completed.
[4]Provide estimates for manpower requirements and authorizations. Provide deltas between requirements and authorizations for each fiscal year.

Contractor Sub-Total						
SUPPORT:[4] Military Officers Enlisted Civilian Contractor Sub-Total						
TRAIN:[4] Military Officers Enlisted Civilian Contractor Sub-Total						
TOTAL						

3.6. Major Automated Information Systems Economic Analysis

3.6.1. Introduction

An automated information system (AIS) is a system of computer hardware, computer software, data and/or telecommunications that performs functions such as collecting, processing, storing, transmitting and displaying information; however, systems that are an integral part of a weapon or weapon system are excluded from this definition. AIS programs that meet the specified dollar thresholds in DoD Instruction 5000.02, Enclosure 3, Table 1, qualify as Major Automated Information System (MAIS) programs. MAIS programs that are subject to review by OSD, at the Information Technology Acquisition Board (ITAB), are designated Acquisition Category (ACAT) IAM. Other MAIS programs, delegated to the head of the DoD Component or the appropriate DoD Component Acquisition Executive, are designated ACAT IAC. In some cases, an ACAT IA program also meets the definition of a Major Defense Acquisition Program (MDAP). In these cases, the USD(AT&L) is the Milestone Decision Authority unless delegated

to a DoD Component, and the statutory requirements that apply to both MAIS programs and MDAPs apply.

DoD Instruction 5000.02, Enclosure 4, Table 2-1, requires that an Economic Analysis be performed in support of the Milestone A, Milestone B, and full-rate production decision (or equivalent) reviews. The purpose of the Economic Analysis is to determine the best AIS program acquisition alternative, by assessing the net costs and benefits of the proposed AIS program relative to the status quo. In general, the best alternative will be the one that meets validated capability needs at the lowest life-cycle cost (measured in net present value terms), and/or provides the most favorable return on investment.

Whenever an Economic Analysis is required, the DoD Component responsible for the program also may be required to provide a DoD Component Cost Analysis, which is an independent estimate of program life-cycle costs. Normally, the Economic Analysis is prepared by the AIS program office, and the DoD Component Cost Analysis is prepared by an office or entity not associated with the program office or its immediate chain of command. The need for a Component Cost Analysis at Milestone A is evaluated for each program in tailoring the oversight process.

The Economic Analysis should be accomplished in accordance with DoD Instruction 7041.3, "Economic Analysis for Decisionmaking." Normally, the DoD Component submits a Final Cost/Benefit Position that resolves the differences between the Economic Analysis and the Component Cost Analysis. Also, the Affordability Assessment should address any differences between the Final Cost/Benefit Position and the funding in the current Future Years Defense Program.

In addition to an Economic Analysis, independent cost estimates are occasionally required for MAIS programs. Per 10 U.S.C. 2445c, MAIS programs where the MDA is USD(AT&L) (ACAT IA) that experience critical program changes must undergo an independent cost estimate prepared by the Director of Cost Assessment and Program Evaluation (CAPE). Independent cost estimates will also be conducted for MAIS programs at any other time considered appropriate by the Director of CAPE, or upon request by USD(AT&L) (see 10 U.S.C. 2334).

3.6.2. Office of Cost Assessment and Program Evaluation Review Procedures

For Acquisition Category IAM programs, both the Economic Analysis and the DoD Component Cost Analysis are subject to independent review and assessment by the Office of the Director of Cost Assessment and Program Evaluation (OD/CAPE).

The purpose of the OD/CAPE's assessment is to provide the Milestone Decision Authority with an independent determination that (1) the estimates of life-cycle costs and benefits are reasonable, traceable, and reflect DoD policy and OD/CAPE guidance on the consideration of life-cycle costs, (2) the return on investment calculation is valid, and (3) the cost estimates are built on realistic program and schedule assumptions.

During the review process, the OD/CAPE staff may engage in discussion with the DoD Components regarding any discrepancies related to MAIS cost estimates and comment on deficiencies regarding the methodology or execution of cost estimates. Furthermore, OD/CAPE staff are authorized to concur with the choice of a cost estimate used to support the acquisition program baseline (APB) as well as in the selection of a proper confidence interval for the MAIS program.

The Congress has required certain risk reporting aspects for MAIS programs. For such programs, the Director of Cost Assessment and Program Evaluation (DCAPE) and the Secretary of the Military Department concerned (or the head of the Defense Agency concerned) must state the confidence level used in establishing a cost estimate, the rationale for selecting the confidence level, and, if the confidence level is less than 80 percent, the justification for selecting the lower confidence level.

The confidence level disclosure shall be included in the ADM approving the APB, and in any other cost estimates for MAIS programs prepared in association with this section.

3.6.2.1. Kick-Off Meeting

The review process normally begins with a kick-off meeting held with OD/CAPE staff, representatives from the Automated Information System (AIS) program office, the DoD Component Cost Analysis Team, and any DoD Component functional or headquarters sponsors. The purpose of the meeting is to reach a common understanding on the expectations for the upcoming activities and events leading to the Information Technology Acquisition Board milestone review. As a starting point, the DoD Component staff and/or sponsors' representatives should review the contents of the most recently approved capability needs documents, and explain any prior analysis (such as a Capabilities-Based Assessment) used to justify the need for a materiel solution (that will be met by the AIS program).

At the kick-off meeting, the DoD Component staff and/or sponsors' representatives also should be prepared to explain the planned approach for the upcoming Economic Analysis. To facilitate this dialogue, the AIS program office should prepare and provide a brief Economic Analysis development plan. The development plan should document the organizational responsibilities, analytic approach, ground rules and assumptions, and schedule for the economic analysis. The development plan should identify the specific alternatives that will be compared in the Economic Analysis. Normally, at least one alternative should be associated with the proposed AIS program, and one alternative should be associated with the status quo (no modernization investment). It may well be the case that the status quo alternative represents an unacceptable mission posture-it may cost too much to sustain, be unable to meet critical capability needs, or be unsupportable due to technological obsolescence. Nevertheless, the status quo concept, applied over the same time frame (Life Cycle) as the proposed AIS program, is used for comparative purposes in the Economic Analysis. The Economic Analysis development plan should document the DoD Component Cost Analysis approach and schedule as well.

As part of the Economic Analysis development plan, the program office should propose the cost element structure that will be used to organize and categorize cost estimates in the Economic Analysis. The cost element structure provides a hierarchal framework of defined cost elements that in total comprise the program life-cycle cost. The cost element structure should include phase-out costs associated with the status quo (legacy or predecessor) system. These costs would be incurred in managing, preserving, and maintaining the operations of the status quo system as it runs parallel to the phasing in of the new system. The status quo phase-out cost elements are not used in the estimate of the status quo alternative. A sample of a generic cost element structure is available from the OD/CAPE staff. OD/CAPE can also provide advice on a consistent approach to net present value and return on investment computations.

3.6.2.2. Use of the Cost Analysis Requirements Description (CARD) for Automated Information System (AIS) Programs

As soon as possible after the kick-off meeting, the draft Cost Analysis Requirements Description (CARD) is provided to the OD/CAPE staff for review. The CARD is used to define and describe the AIS program for purposes of preparing both the Economic Analysis and the DoD Component Cost Analysis. For an AIS program, the CARD typically would address the following elements:

- Program description;
- Program operational concept;
- Program data management requirements;
- Program quantity requirements;
- Program manpower requirements;
- Program fielding strategy;
- Program milestone schedule; and
- Program acquisition plan or strategy.

Procedures for the preparation of the CARD are described in DoD Instruction 5000.02, Enclosure 7, paragraph 2. Additional guidelines on CARD preparation are found in DoD 5000.4 M, "DoD Cost Analysis Guidance and Procedures," Section 1. However, these guidelines are for the most part oriented toward weapon systems, and may need to be tailored somewhat for automated information systems. The system description in the CARD should address both hardware and software elements. The CARD should describe each major hardware item (computers, servers, etc.), noting those items that are to be developed, and those items that are off-the-shelf. The CARD also should describe each software configuration item (including applications as well as support software) and identify those items that are to be developed. For software items to be developed, the CARD should provide (1) some type of sizing information (such as counts of source lines of code, function points, or Reports, Interfaces, Conversions and Enhancements (RICE)-Forms and Workflows (FW) (RICE-(FW) objects) suitable for cost estimating, and (2) information about the programming language and environment. In addition, the CARD should describe any special (physical, information, or operations) system security requirements, if applicable.

Clearly, much of the information needed for the CARD is often available in other program documents. The CARD should stand-alone as a readable document, but can make liberal use of appropriate references to the source documents to minimize redundancy and effort. In such cases, the CARD should briefly summarize the information pertinent to the Economic Analysis in the appropriate section of the CARD, and provide a reference to the source document.

3.6.2.3. Office of Cost Assessment and Program Evaluation's CARD Review and Assessment

To facilitate the OD/CAPE review and assessment, the DoD Component's Economic Analysis and Cost Analysis teams should provide written documentation early enough to permit a timely report to the Overarching Integrated Product Team (OIPT) and Information Technology Acquisition Board. Normally, the documentation is provided 30 to 60 days prior to the OIPT meeting. The documentation serves as an audit trail of source data, methods, and results. The documentation should be easy to read, complete and well organized to allow any reviewer to understand the estimate fully. The documentation also serves as a valuable reference for future cost analysts, as the program moves from one acquisition milestone to the next.

After review of the documentation, the OD/CAPE staff provides feedback to the program office and DoD Component staff. Subsequently, the OD/CAPE staff prepares a written report containing the findings of their independent assessment to the Milestone Decision Authority. Depending on the circumstances, the report may contain recommended cost and benefits positions, and it may raise funding or schedule issues. The expectation is that any issues raised have already emerged in prior discussions and that the final OD/CAPE report should not contain any surprises.

3.7. Principles for Life-Cycle Cost Estimates

3.7. Principles for Life-Cycle Cost Estimates

Section 3.4.3 of this Guidebook primarily focused on procedures associated with life-cycle cost estimates, which are subject to review by the Office of Cost Assessment, for major defense acquisition programs. The estimate is prepared in support of major milestone or other program reviews held by the Defense Acquisition Board. This section is intended to be more generally applicable and somewhat more analytic in nature. It describes a recommended analytic approach for planning, conducting, and documenting a life-cycle cost estimate for a defense acquisition program (whether or not the estimate is subject to Office of Cost Assessment review). Much of the discussion in this section was written with the less experienced cost analyst in mind.

The recommended analytic approach for preparing a life-cycle cost estimate is shown in Figure 3.7.F1:

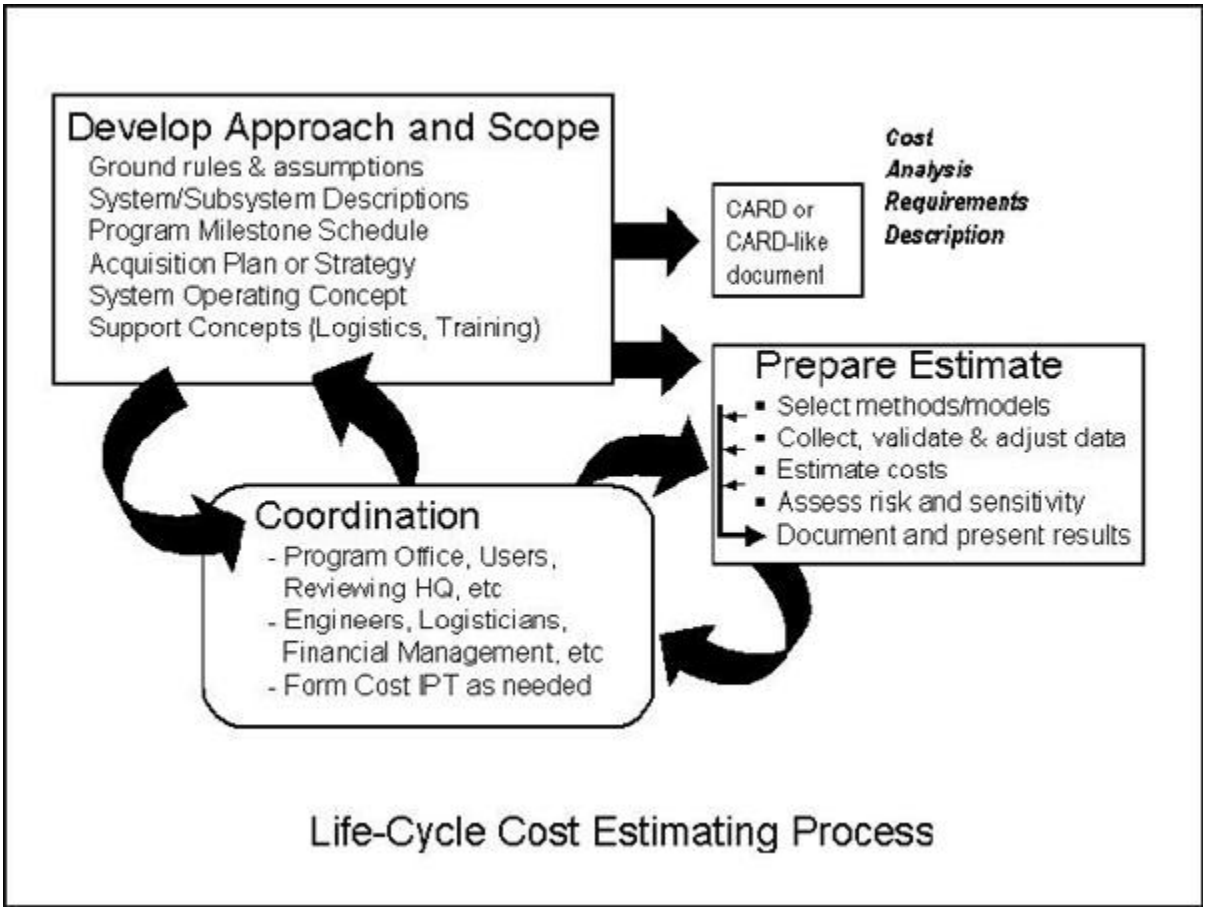


Figure 3.7.F1. A Recommended Analytic Approach for Life-Cycle Cost Estimates

The next few sections describe this process.

3.7.1. Develop Approach and Scope

The first step in preparing a credible cost estimate is to begin with the development of a sound analytic approach. During this planning phase, critical ground rules and assumptions are established, the scope of the estimate is determined, and the program to be costed is carefully defined and documented. The program definition includes not only a technical and physical description of the system (and perhaps major subsystems), but also a description of the system's program schedule, acquisition strategy, and operating and support concepts. In some cases, it is necessary to state explicitly the costs to be included, and the costs to be excluded. For example, when systems have complex interfaces with other systems or programs (that are outside the scope of the system being costed), the interfaces should be carefully defined.

For programs that will be reviewed by the Office of Cost Assessment, the program office is required to define its program in a comprehensive formal written document known as a Cost

Analysis Requirements Description (CARD). The format for this document is briefly summarized in section 3.4.4.1 of this Guidebook, and is completely described in DoD 5000.4 M, "DoD Cost Analysis Guidance and Procedures," Section1. For programs preparing a cost estimate not subject to Office of Cost Assessment review, the CARD format, with appropriate tailoring, nevertheless provides a useful and flexible framework for developing a written program description suitable for a life-cycle cost estimate. Much of the necessary information to prepare a written program description can be extracted and synthesized from common program source documents and contract specifications. The written program description should stand-alone as a readable document, but can make liberal use of suitable references to the source documents to minimize redundancy and effort.

It is important that the analytic approach to the cost estimate be documented and reviewed by all potentially interested parties, before the actual work on preparing the cost estimate begins. This helps ensure that there are no false starts or misunderstandings later in the process.

3.7.1.1. Work Breakdown Structure (WBS)

Part of the system definition typically includes the program work breakdown structure. The program WBS is a hierarchy of product-oriented elements (hardware, deliverable software, data, and services) that collectively comprise the system to be developed or produced. The program WBS relates the elements of work to each other and to the end product. The program WBS is extended to a contract WBS that defines the logical relationship between the elements of the program and corresponding elements of the contract work statement. The WBS provides the framework for program and technical planning, cost estimating, resource allocation, performance measurement, technical assessment, and status reporting. In particular, the contract WBS provides the reporting structure used in contract management reports (such as contract performance reports (see section 11.3.1.4.1) or reports in the Contractor Cost Data Reporting system (see section 3.4.4.2.1). Further information about the WBS can be found in MIL-HDBK-881A, Work Breakdown Structures for Defense Materiel Items, which is available at the Defense Cost and Resource Center web site.

A sample of the WBS for an air-to-air tactical missile is provided in Figure 3.7.1.1.F1

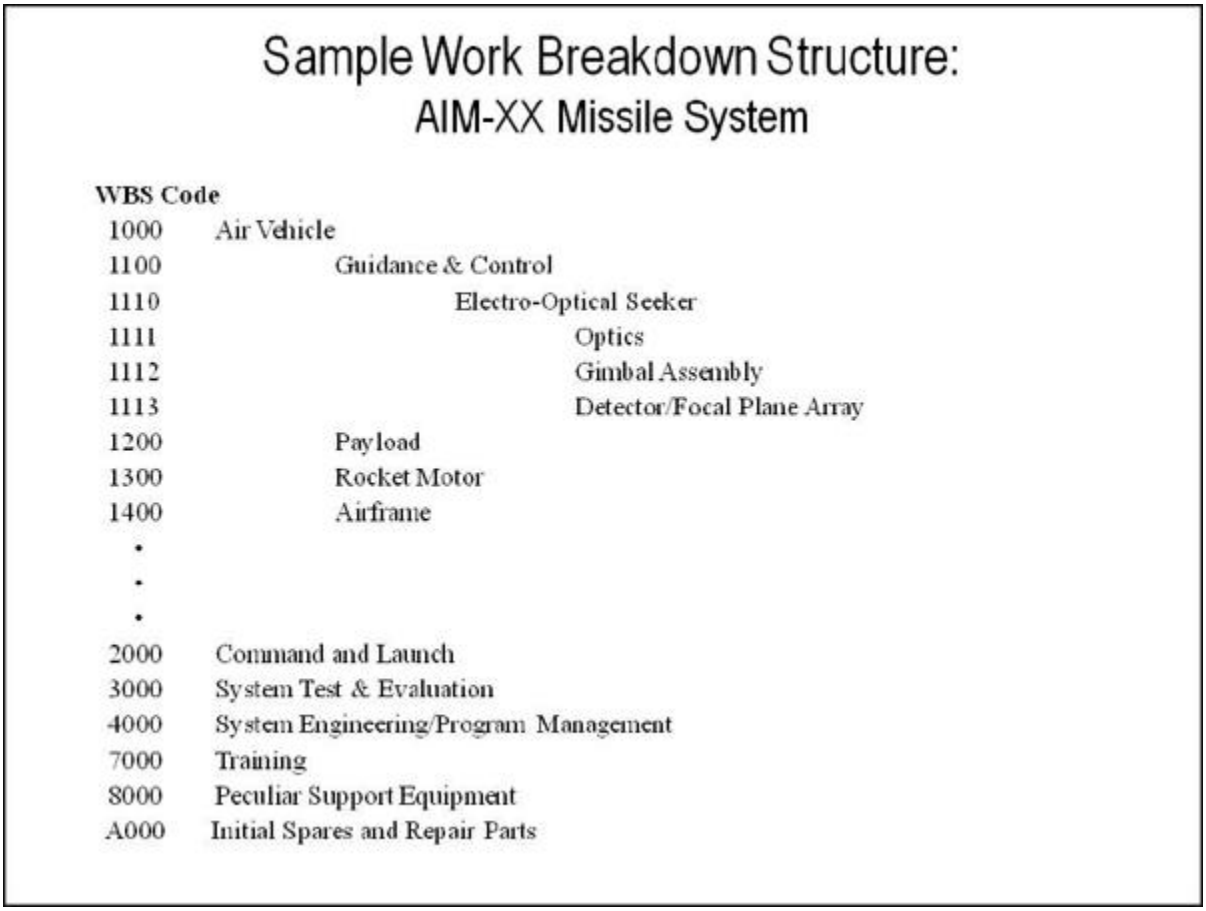


Figure 3.7.1.1.F1. Sample Work Breakdown Structure

3.7.1.2. Cost Estimating Functional Categories

In most cost estimates, selected WBS elements (usually high cost) often are further broken down into functional categories. A typical structure for the functional categories is provided in Figure 3.7.1.2.F1. In the tactical missile example discussed in the last section, most likely the cost estimate for the Airframe WBS element would be broken down by functional category, whereas the cost estimate for the Initial Spares and Repair Parts WBS element most likely would be estimated at the level of total cost, and not by functional category.

Standard terms and definitions for the various functional categories were developed to support the Cost and Software Data Reporting system (see section 3.4.4.2). The terms and definitions used in Figure 3.7.1.2.F1 can be found in the following:

- DoD 5000.04-M-1, "Cost and Software Data Reporting (CSDR) Manual"
- Data Item Description DI-FNCL-81565B, "Cost Data Summary Report (DD Form 1921)"

- Data Item Description DI-FNCL-81566B, "Functional Cost-Hour Report (DD Form 1921-1)"

All of these are available at the Defense Cost and Resource Center web site.

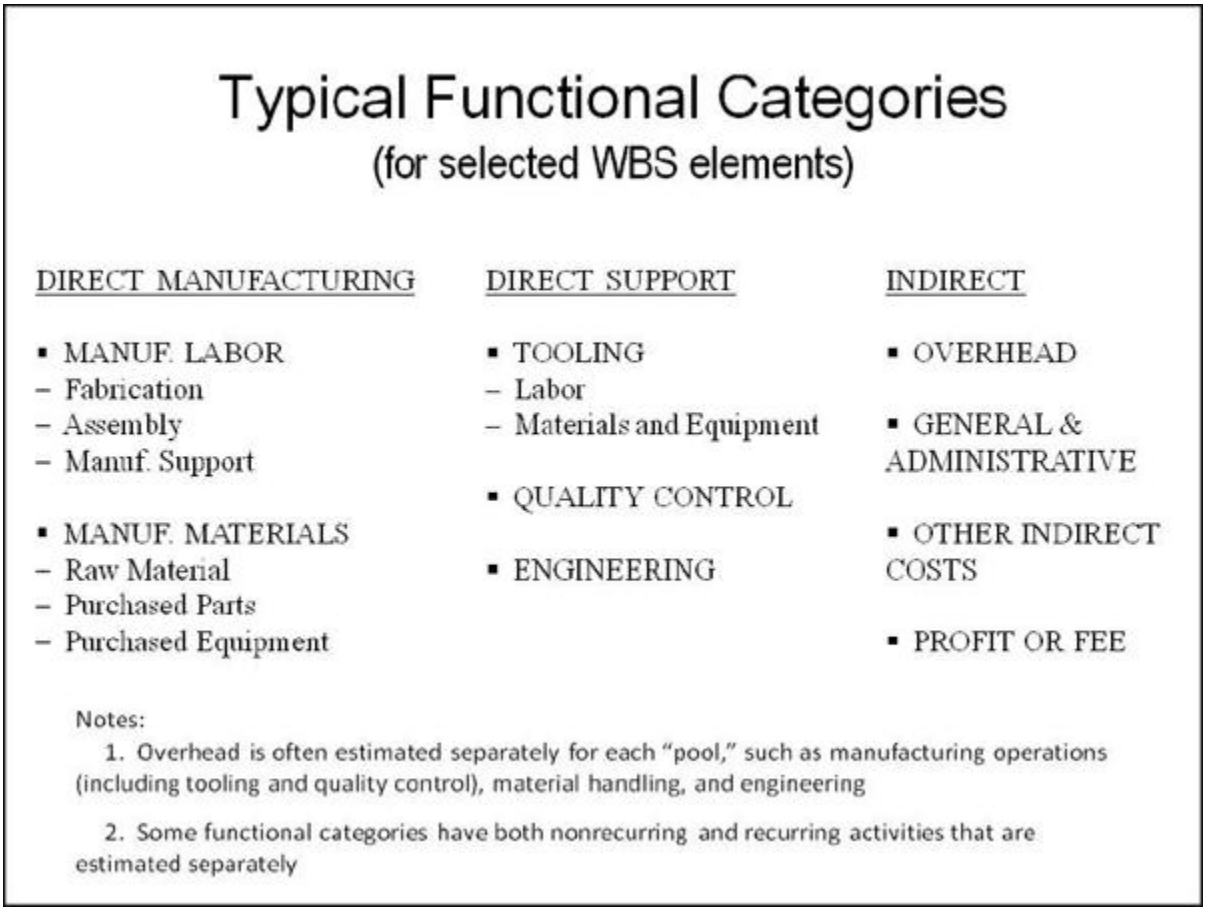


Figure 3.7.1.2.F1. Functional Categories for Cost Estimating

3.7.1.3. Operating and Support (O&S) Cost Element Structure

Another step in developing the analytic approach to the cost estimate is establishing the cost element structure that will be used as the format for the O&S cost estimate. The cost element structure describes and defines the specific elements to be included in the O&S cost estimate in a disciplined hierarchy. Using a formal cost element structure (prepared and coordinated in advance of the actual estimating) identifies all of the costs to be considered, and organizes the estimate results. The cost element structure is used to organize an O&S cost estimate similar to the way that a work breakdown structure is used to organize a development or procurement cost estimate. The intent is to capture all costs of operating, maintaining, and supporting a fielded system (and its associated manpower and facilities). A notional portrayal of these costs,

organized into a cost element structure format, is provided in Figure 3.7.1.3.F1. Note that the use of a cost element structure provides considerably more detail than simply using budget appropriation categories (operations and maintenance, military personnel).

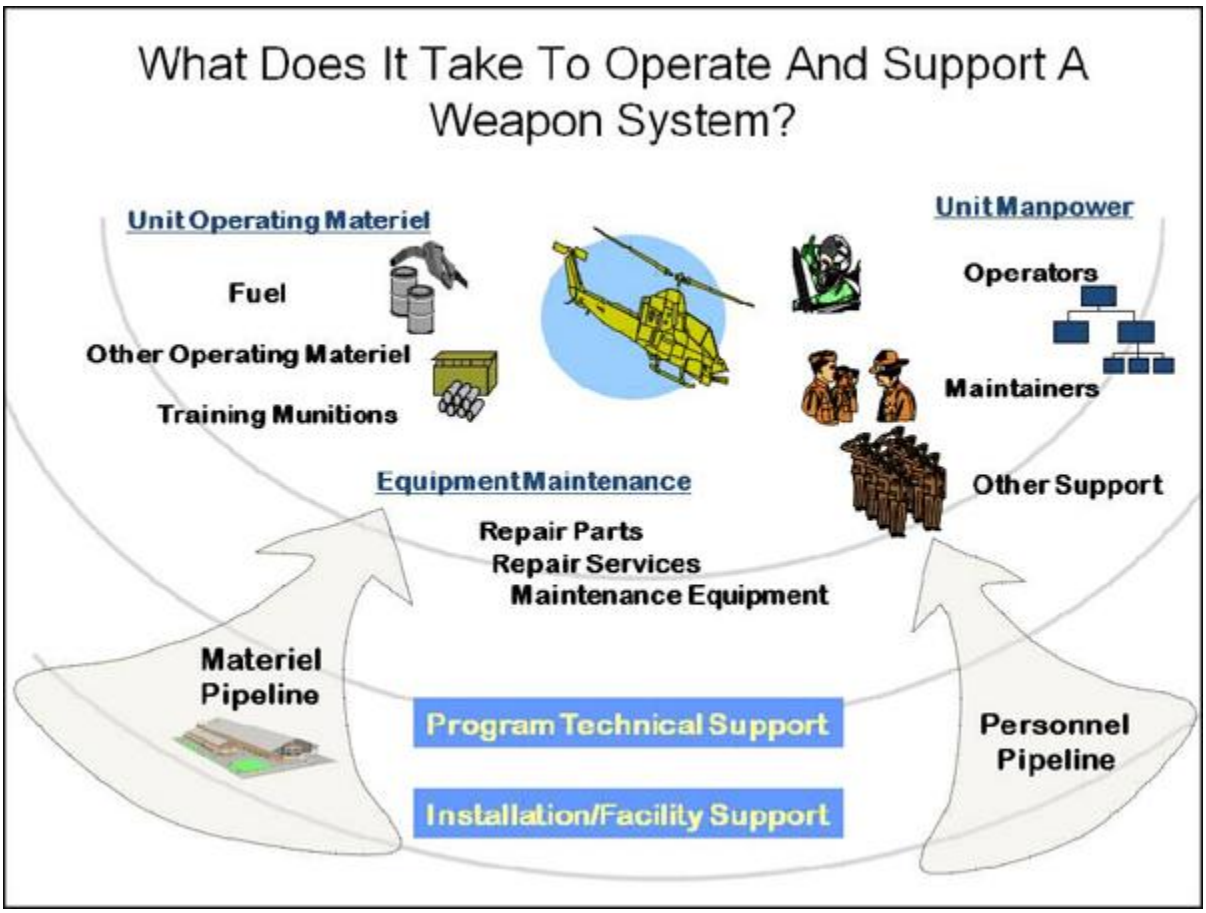


Figure 3.7.1.3.F1. O&S Costs Organized by a Cost Element Structure

A standard cost element structure used by the Office of Cost Assessment was introduced in section 3.1.3.3. Details can be found in the OSD CAIG O&S Cost-Estimating Guide. Although each DoD Component (military department or defense agency) may have its own preferred cost element structure, it is expected that each DoD Component will have a cross walk or mapping so that any presentation to the Office of Cost Assessment can be made using the standard structure.

3.7.2. Prepare the Estimate

This section describes the typical steps in preparing a life-cycle cost estimate. The discussion summarizes the steps entailed in selecting estimating techniques or models, collecting data, estimating costs, and conducting sensitivity or risk analysis.

In addition, the importance of good documentation of the estimate is explained.

3.7.2.1. Select Methods and/or Models

A number of techniques may be employed to estimate the costs of a weapon system. The suitability of a specific approach will depend to a large degree on the maturity of the program and the level of detail of the available data. Most cost estimates are accomplished using a combination of the following estimating techniques:

- **Parametric.** The parametric technique uses regression or other statistical methods to develop Cost Estimating Relationships (CERs). A CER is an equation used to estimate a given cost element using an established relationship with one or more independent variables. The relationship may be mathematically simple or it may involve a complex equation (often derived from regression analysis of historical systems or subsystems). CERs should be current, applicable to the system or subsystem in question, and appropriate for the range of data being considered.
- **Analogy.** An analogy is a technique used to estimate a cost based on historical data for an analogous system or subsystem. In this technique, a currently fielded system, similar in design and operation to the proposed system, is used as a basis for the analogy. The cost of the proposed system is then estimated by adjusting the historical cost of the current system to account for differences (between the proposed and current systems). Such adjustments can be made through the use of factors (sometimes called scaling parameters) that represent differences in size, performance, technology, and/or complexity. Adjustment factors based on quantitative data are usually preferable to adjustment factors based on judgments from subject-matter experts.
- **Engineering Estimate.** With this technique, the system being costed is broken down into lower-level components (such as parts or assemblies), each of which is costed separately for direct labor, direct material, and other costs. Engineering estimates for direct labor hours may be based on analyses of engineering drawings and contractor or industry-wide standards. Engineering estimates for direct material may be based on discrete raw material and purchase part requirements. The remaining elements of cost (such as quality control or various overhead charges) may be factored from the direct labor and material costs. The various discrete cost estimates are aggregated by simple algebraic equations (hence the common name "bottoms-up" estimate). The use of engineering estimates requires extensive knowledge of a system's (and its components') characteristics, and lots of detailed data.
- **Actual Costs.** With this technique, actual cost experience or trends (from prototypes, engineering development models, and/or early production items) are used to project estimates of future costs for the same system. These projections may be made at various levels of detail, depending on the availability of data. Cost estimates that support a full-rate production milestone decision should be based on actual cost data to the greatest extent possible. A common mistake is to use contract prices as a substitute for actual cost experience. Contract prices should not be used to project future costs (even when firm-fixed price) unless it is known that the contract prices are associated with profitable

ventures, and that it is reasonable to assume that similar price experience will be obtained for subsequent contracts.

In many instances, it is a common practice to employ more than one cost estimating method, so that a second method can serve as a cross-check to the preferred method. Analogy estimates are often used as cross-checks, even for estimates of mature systems based on actual costs.

The next two sections provide two illustrative examples of common cost estimating techniques.

3.7.2.1.1. Example #1-Cost Estimating Relationship

An exemplar cost estimating relationship is provided in Figure 3.7.2.1.1.F1. The relationship is used to estimate production costs for a component of a tactical missile, using various technical characteristics as independent variables. Developing a good relationship requires not only sound statistical practice, but also considerable experience and insight on the part of the cost analyst. It also requires detailed and well-understood data.

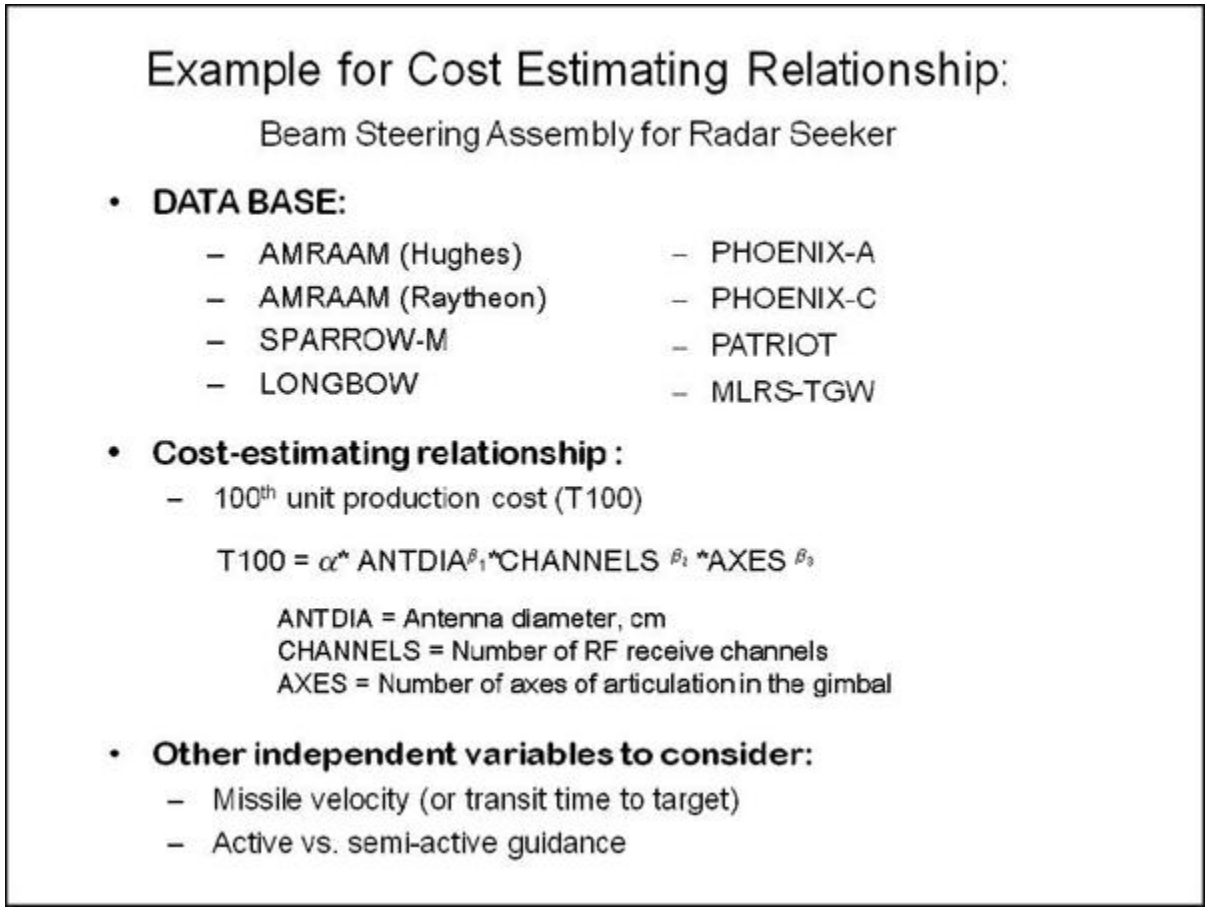


Figure 3.7.2.1.1.F1. Illustrative Cost Estimating Relationship

3.7.2.1.2. Example #2-Analogy

An exemplar cost estimate by analogy is provided in Figure 3.7.2.1.2.F1. In this case, an estimate for one of the Operating and Support (O&S) cost elements (depot level reparables) for a future aircraft system is made by direct analogy to a predecessor aircraft system with a similar mission. Note that the analogy uses scaling parameters for operating (i.e., flying) hours, reliability, and system unit cost. In many analogy estimates, unit cost is often used as a proxy for complexity.

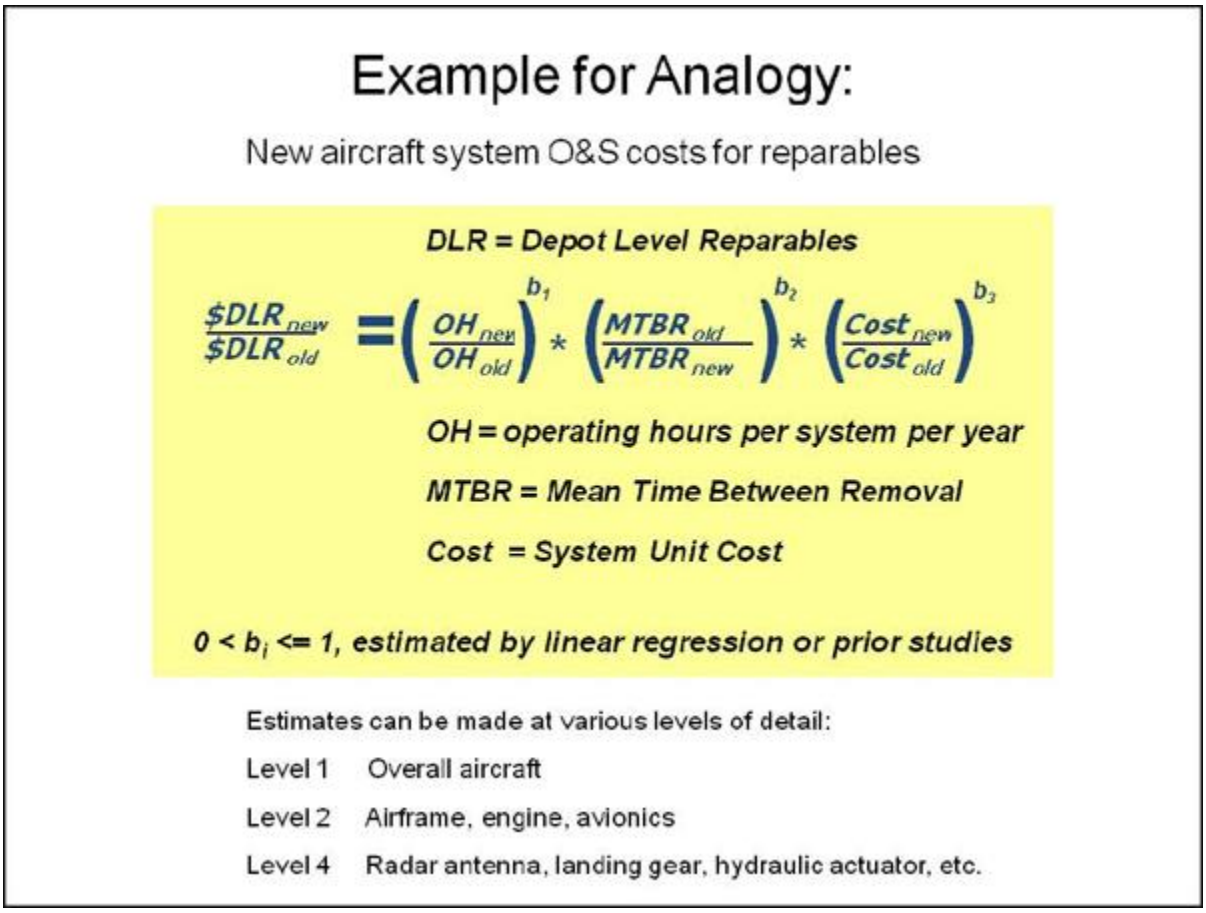


Figure 3.7.2.1.2.F1. Illustrative Cost Estimate by Analogy

3.7.2.2. Collect, Validate, and Adjust Data

There are many possible sources of data that can be used in cost estimates. Regardless of the source, the validation of the data (relative to the purpose of its intended use) always remains the responsibility of the cost analyst. In some cases, the data will need to be adjusted or normalized. For example, in analogy estimates, the reference system cost should be adjusted to account for any differences in system characteristics (technical, physical, complexity, or hardware cost) or operating environment between the reference system and the proposed system being costed.

3.7.2.2.1. Acquisition Cost Data

Actual cost experience on past and current acquisition programs often forms the basis of estimates of future systems. The Cost and Software Data Reporting (CSDR) system is the primary means within the Department of Defense to systematically collect data on the development and production costs and other resource usage incurred by contractors in performing DoD acquisition program contracts associated with major defense acquisition programs. CSDR consists of two components: Contractor Cost Data Reporting (CCDR), and Software Resources Data Reporting (SRDR).

CCDR reports provide for each contract a display of incurred costs to date and estimated incurred costs at completion by elements of the Work Breakdown Structure, with nonrecurring costs and recurring costs separately identified. In addition, in some cases, CCDR reports can display incurred costs to date and estimated incurred costs at completion by functional category (manufacturing labor, engineering, etc.). Where appropriate, a functional category is broken out by direct labor hours, direct material, overhead, and other indirect.

SRDR reports are used to collect software metrics from the contracts associated with major software development efforts for major defense acquisition programs. Data collected from applicable contracts include the type and size of the software applications (configuration items), schedule, and labor resources associated with the software development.

DoD 5000.04-M-1, "Cost and Software Data Reporting (CSDR) Manual," provides report formats and definitions, specific report examples, and other related information. The CSDR Manual can be found at the Defense Cost and Resource Center web site. The DCARC is the OSD office responsible for administering the CCDR system. Access to CSDR data is readily provided by the DCARC to DoD government cost analysts, and sponsored support contractors, who are registered users.

It is not unusual for cost analysts to rely on other sources of cost data beyond CSDR reports. Analysts often also use Contract Performance Reports or other Earned Value Management reports. Sometimes analysts resort to ad hoc data calls to program offices, contractors, and the appropriate Defense Contract Management Agency field organizations.

3.7.2.2.2. Operating and Support (O&S) Cost Data

Historical O&S cost data for currently fielded systems are available from the Visibility and Management of Operating and Support Costs (VAMOSC) data system managed by each DoD military service. The data can be displayed in several different formats, including the Office of Cost Assessment standard cost element structure described previously. Data can be obtained for entire systems, or at lower levels of detail. VAMOSC provides not only cost data, but related non-cost data (such as operating tempo or maintenance man-hours) as well. This type of data is useful for analogy estimates (between proposed systems and appropriate predecessor or reference systems) and for "bottoms-up" engineering estimates (for fielded systems or

components, possibly adjusted for projected reliability and maintainability growth). VAMOSC data should always be carefully examined before use in a cost estimate. The data should be displayed over a period of a few years (not just a single year), and stratified by different sources (such as major command or base). This should be done so that abnormal outliers in the data can be identified, investigated, and resolved as necessary.

3.7.2.3. Estimate Costs

With the completion of the steps described earlier in this chapter, the actual computations of the cost estimate can begin. It is important to assess critically the outputs from the estimating methods and models, drawing conclusions about reasonableness and validity. Peer review is often helpful at this point. For complex cost estimates, with many elements provided from different sources, considerable effort and care are needed to deconflict and synthesize the various elements.

3.7.2.4. Assess Risk and Sensitivity

For any system, estimates of future life-cycle costs are subject to varying degrees of uncertainty. The overall uncertainty is not only due to uncertainty in cost estimating methods, but also due to uncertainties in program or system definition or in technical performance. Although these uncertainties cannot be eliminated, it is useful to identify associated risk issues and to attempt to quantify the degree of uncertainty as much as possible. This bounding of the cost estimate may be attempted through sensitivity analyses or through a formal quantitative risk analysis.

Sensitivity analysis attempts to demonstrate how cost estimates would change if one or more assumptions change. Typically, for the high-cost elements, the analyst identifies the relevant cost-drivers, and then examines how costs vary with changes in the cost-driver values. For example, a sensitivity analysis might examine how maintenance manning varies with different assumptions about system reliability and maintainability values, or how system manufacturing labor and material costs vary with system weight growth. In good sensitivity analyses, the cost-drivers are not changed by arbitrary plus/minus percentages, but rather by a careful assessment of the underlying risks. Sensitivity analysis is useful for identifying critical estimating assumptions, but has limited utility in providing a comprehensive sense of overall uncertainty.

In contrast, quantitative risk analysis can provide a broad overall assessment of variability in the cost estimate. In risk analysis, selected factors (technical, programmatic and cost) are described by probability distributions. Where estimates are based on cost models derived from historical data, the effects of cost estimation error may be included in the range of considerations included in the cost risk assessment. Risk analysis assesses the aggregate variability in the overall estimate due to the variability in each input probability distribution, typically through Monte-Carlo simulations. It is then possible to derive an estimated empirical probability distribution for the overall life-cycle cost estimate. This allows the analyst to describe the nature and degree of variability in the estimate.

Sensitivity and risk analyses also have uses beyond addressing the uncertainty in cost estimates. They also can be used to help better understand what can go wrong with a program, and focus appropriate management attention to risk areas that are concerns. The history of DoD weapon system acquisition would indicate that cost growth and schedule delays can occur as a direct result of one or more of the following concerns:

- Immaturity of critical technologies at the start of development
- Inadequate understanding of design challenges at the start of development (often due to the absence of prototyping)
- Requirements uncertainty, instability, or creep
- Failure to acknowledge (or deal with) funding shortfalls
- Funding instability in the programming, budgeting or appropriations process
- Failure to detect (or deal with) unrealistic contractor cost proposals in competitive source selections (from either the prime or major subcontractors)
- Excessive concurrency between development and procurement schedules
- Inadequate understanding of software development size and integration challenges
- Failure to achieve design stability by the time of the critical design review
- Failure to achieve stable manufacturing processes by the time of early production

3.7.2.5. Document and Present Results

A complete cost estimate should be formally documented. The documentation serves as an audit trail of source data, methods, and results. The documentation should be easy to read, complete and well organized-to allow any reviewer to understand the estimate fully. The documentation also serves as a valuable reference for future cost analysts, as the program moves from one acquisition milestone to the next.

The documentation should address all aspects of the cost estimate: all ground rules and assumptions; the description of the system and its operating and support concepts; the selection of cost estimating methods; data sources; the actual estimate computations; and the results of any sensitivity or risk analyses. The documentation for the ground rules and assumptions, and the system description, should be written as an updated (final) version of the Cost Analysis Requirements Description (CARD) or CARD-like document described earlier. The documentation for the portion of the cost estimate dealing with data, methods, and results often is published separately from the CARD or CARD-like document, but if that is the case, the two documents should be completely consistent.

3.7.3. Coordination

Managing the preparation of a life-cycle cost estimate requires continual coordination among all of the stakeholders. Normally, cost estimates are sponsored by a system program office and are prepared by a multi-disciplinary team with functional skills in financial management, logistics, engineering, and other talents. The team also should include participants or reviewers from major affected organizations, such as the system's operating command, product support center,

maintenance depot, training center or command, and so forth. Typically, the analytic approach to the cost estimate is documented in a written study plan that includes a master schedule (of specific tasks, responsible parties, and due dates). For sufficiently complex efforts, the estimating team may be organized as a formal Integrated Product Team. Throughout the preparation of the estimate, coordination with all interested parties remains important. Frequent in-progress reviews or meetings are usually a good practice.

For independent cost estimates, the team may be smaller and less formal, but the basic principle-complete and continual coordination of the cost estimate with all interested parties-still applies.

3.7.4. Further Information and Training

The Acquisition Community Connection website has additional information on cost analysis.

In addition, the Defense Acquisition University offers the following courses in residence:

- BCF 106 -- Fundamentals of Cost Analysis;
- BCF 107 -- Applied Cost Analysis;
- BCF 204 -- Intermediate Cost Analysis;
- BCF 206 -- Cost/Risk Analysis;
- BCF 208 -- Software Cost Estimating;
- BCF 215 -- Operating and Support Cost Analysis; and

As well as the following courses as on-line continuous learning modules:

- CLB 007 - - Cost Analysis
- CLM016 - - Cost Estimating
- CLB024 - - Cost Risk Analysis Introduction

In addition, each year the Cost Assessment Office sponsors a Department of Defense Cost Analysis Symposium. This symposium includes presentations from government and support contractor cost analysts concerning best practices and state-of-the-art in cost estimating. The Symposium also features senior distinguished speakers and panelists from government, industry, and academia. Further information may be found at the DoD Cost Analysis Symposium web site.

DEFENSE ACQUISITION GUIDEBOOK
Chapter 4 -- Systems Engineering

4.0. Overview

The purpose of this chapter is to facilitate compliance with mandatory systems engineering direction outlined in Department of Defense (DoD) policy. The chapter provides the definition of systems engineering accepted by the Department, outlines DoD guidance on systems engineering, and explains expectations for completing the Systems Engineering Plan (SEP). The chapter describes standard systems engineering processes and how they apply to the DoD acquisition system. It addresses the systems engineering principles that a program manager should apply to achieve a balanced system solution.

4.0.1. Contents

This overview discusses definitions of systems engineering and presents excerpts from DoD policy outlining expectations for systems engineering in acquisition programs. Following the overview, the chapter includes the following six sections:

Section 4.1, Systems Engineering in DoD Acquisition, provides perspective on the use of systems engineering processes to translate user-defined capabilities into engineering specifications and outlines the role of the program manager in integrated system design activities.

Section 4.2, Systems Engineering Processes: How Systems Engineering Is Conducted, discusses systems engineering processes. It groups them into technical management processes and technical processes categories. This section also contains a discussion on the use of standards and tailoring of process models, and explains what to expect from the contractor's systems engineering process.

Section 4.3, Systems Engineering in the System Life Cycle, provides an integrated technical framework for systems engineering activities throughout the acquisition phases of a system's life cycle, highlighting the particular systems engineering inputs, activities, products, technical reviews, and outputs of each acquisition phase.

Section 4.4, Systems Engineering Design Considerations, discusses the many design considerations to take into account across the spectrum of systems engineering activities. These considerations include: accessibility, commercial off-the-shelf (COTS) items; corrosion prevention and control; critical safety items; disposal and demilitarization; diminishing manufacturing sources and material shortages; environment, safety, and occupational health; human systems integration; insensitive munitions; interoperability; open systems design; parts management; program protection; quality; producibility; reliability; availability, and maintainability; software; standardization; supportability; survivability; and susceptibility; and unique identification of items.

Section 4.5, Systems Engineering Execution: Key Systems Engineering Tools and Techniques, includes the important technical, cost, and schedule oversight methods and techniques used in the technical management and technical processes. This section also discusses general knowledge management tools.

Section 4.6, Systems Engineering Resources, provides references to many systems engineering resources that already exist across the government, industry, and academia. Links to resources are incorporated throughout the text of this chapter, as appropriate. This section lists available resources, including standards and models, handbooks, guides, and additional references.

4.0.2. Definition of Systems Engineering

Numerous definitions of systems engineering exist. DoD has adopted the following formal definition, derived from EIA/IS 632, "Processes for Engineering a System" (available for purchase):

Systems engineering is an interdisciplinary approach encompassing the entire technical effort to evolve and verify an integrated and total life cycle balanced set of system, people, and process

solutions that satisfy customer needs. Systems engineering is the integrating mechanism across the technical efforts related to the development, manufacturing, verification, deployment, operations, support, disposal of, and user training for systems and their life cycle processes. Systems engineering develops technical information to support the program management decision-making process.

For DoD, systems engineering is the set of overarching processes that a program team applies to develop an operationally effective and suitable system from a stated capability need. Systems engineering processes apply across the acquisition life cycle (adapted to each phase) and serve as a mechanism for integrating capability needs, design considerations, design constraints, and risk, as well as limitations imposed by technology, budget, and schedule. The systems engineering processes should be applied during concept definition and then continuously throughout the life cycle.

Systems engineering is a broad topic that includes hardware, software, and human systems. It is an interdisciplinary approach for a structured, disciplined, and documented technical effort to simultaneously design and develop systems products and processes for creating and integrating systems (hardware, software, and human) to satisfy the operational needs of the customer. It transforms needed operational capabilities into an integrated system design through concurrent consideration of all life cycle needs. As systems become larger and more complex, the design, development, and production of such systems or systems of systems (SoS) require the integration of numerous activities and processes. Systems engineering is the approach to coordinating and integrating all these acquisition life cycle activities. It integrates diverse technical management processes to achieve an integrated systems design.

4.0.3. DoD Policy and Guidance on Systems Engineering

The Department recognizes that a well-executed systems engineering (SE) approach is essential to achieving an integrated, balanced system solution. DoD Directive 5000.1, The Defense Acquisition System, directs that:

Acquisition programs shall be managed through the application of a systems engineering approach that optimizes total system performance and minimizes total ownership costs. A modular open-systems approach shall be employed, where feasible.

DoD Instruction 5000.02, Enclosure 12, paragraph 1, directs the use of systems engineering across the acquisition life cycle:

Rigorous systems engineering discipline is necessary to ensure that the Department of Defense meets the challenge of developing and maintaining needed warfighting capability. Systems engineering provides the integrating technical processes to define and balance system performance, cost, schedule, and risk within a family-of-systems and systems-of-systems context. Systems engineering shall be embedded in program planning and be designed to support the entire acquisition life cycle.

In addition, the DoD Instruction 5000.02, Enclosure 12, paragraph 2, directs that:

Program managers shall prepare a Systems Engineering Plan (SEP) for each milestone review, beginning with Milestone A. The SEP at Milestone B and later shall support the Acquisition Strategy. The SEP shall describe the program's overall technical approach, including key technical risks, processes, resources, metrics, and applicable performance incentives. It shall also detail the timing, conduct, and success criteria of technical reviews.

The Milestone Decision Authority (MDA) shall be the approval authority for the SEP. For programs where the USD(AT&L) is the MDA, DoD Components shall submit the SEPs to the Director, Software and Systems Engineering (SSE) [effective 22 May 2009, the Director, Systems Engineering (SE)], at least 30 days before the scheduled Defense Acquisition Board (DAB)/Information Technology Acquisition Board (ITAB) milestone review.

For all other programs (for which the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) is not the MDA), the Component Acquisition Executive (CAE) will designate the SEP approval authority and prescribe submittal instructions.

4.1 Systems Engineering Overview

4.1.1. Systems Engineering in DoD Acquisition

Balanced system solutions are best achieved by applying established systems engineering processes to the planning, development, and sustainment of a system or a system-of-systems (SoS) acquisition in an Integrated Product and Process Development (IPPD) framework.

Systems engineering offers a technical framework to enable sound decision making relative to trade studies, system performance, risk, cost, and schedule. The successful instantiation of proven, disciplined systems engineering processes results in a total system solution that is adaptive to changing technical, production, and operating environments and to the needs of the

use and is balanced among the multiple requirements, design considerations, design constraints, and program budgets.

Table 4.1.1.T1 shows how the roles of the Program Manager and the program systems engineer relate in the context of the system life-cycle processes.

Life-cycle Processes	Program Manager	Chief / Systems Engineer
Stakeholder Management	Primary	Support
Technical Planning	Support	Primary
Decision Analysis	Primary	Support
Technical Assessment (Includes Program Status: Technical Progress, Schedule & Cost Management)	Shared	Shared
Configuration Management	Primary	Support
Data Management	Primary	Support
Requirements Management	Support	Primary
Contract Management	Primary	Support
Requirements Analysis	Support	Primary
Architecture Design	Support	Primary
Implementation	Support	Primary
Risk Management	Primary	Support
Interface Management	Support	Primary
Integration	Support	Primary
Verification	Support	Primary
Validation	Shared	Shared

Table 4.1.1.T1. Role of Systems Engineering in System Life-cycle Processes

The application of rigorous system engineering discipline is paramount to the Department's ability to meet the challenge of developing and maintaining needed warfighting capability. Rigorous system engineering should be included in systems acquisition contracting efforts (i.e., Request for Proposal and Source Selection) to integrate SE requirements. The Guide for

Integrating Systems Engineering into DoD Acquisition Contracts provides guidance and best practices to implement SE policy initiatives in DoD Instruction 5000.02, Enclosure 12, and Systems Engineering Processes on any systems acquisition contracts.

4.1.2. Participants in Systems Engineering

4.1.2. Participants in Systems Engineering

Participants in systems engineering include but are not limited to:

- Program Manager (and other program personnel)
- Program Executive Officer (PEO) Lead or Chief Systems Engineer
- Program Office Level Lead or Chief Systems Engineer
- Program Office Level Test and Evaluation (T&E) Lead
- Program Office Level Lead Logistics Manager
- Systems Engineering Working-Level Integrated Product Team (See also)
- Technical Authority (that is, Functional Leads).

The program manager has the critical role of establishing and implementing a systems engineering approach that includes all stakeholders and leads all participants to translate operational needs and capabilities into technically feasible, affordable, and operationally effective and suitable increments of a system. The systems engineering approach should permeate concept definition, technology/manufacturing maturation, competitive prototyping, design, production, test and evaluation, and life-cycle system support.

Program managers exercise leadership, decision-making, and oversight throughout the system life cycle. Implementing a systems engineering approach adds discipline to the process and provides the program manager with the information necessary to make valid trade-off decisions (see section 2.2.1) to balance cost, schedule, and performance throughout a program's life cycle.

4.1.2.1. Systems Engineering Working-Level Integrated Product Team (SE-WIPT)

Systems engineering is typically implemented through multidisciplinary teams of subject matter experts (SMEs) (often formally chartered as an Integrated Product Team (IPT)) and through an SE-WIPT. The SE-WIPT translates user-defined capabilities into operational system specifications consistent with cost, schedule, and performance constraints. (See the DoD Directive 5000.01 and Guidebook section 11.5 discussions of Knowledge-Based Acquisition).

4.1.2.2. Lead or Chief Systems Engineer

Per DoDI 5000.02, Enclosure 12, each PEO, or equivalent, shall have a lead or chief systems engineer in charge of reviewing assigned programs' SEPs and overseeing their implementation. This lead or chief systems engineer shall also assess the performance of the subordinate lead or chief systems engineers assigned to individual programs in conjunction with the PEO and program manager. Additionally, each program office should have a lead or chief systems engineer to implement the systems engineering process. Personnel from non-systems engineering organizations or from outside the program management structure are often required to support activities related to systems engineering. Most program personnel should see themselves as participants in the systems engineering processes. Systems engineering activities include defining architectures and capabilities (CJCS Instruction 3170.01), and conducting functional analyses. Warfighters, sponsors, maintainers, and planners also actively participate throughout the systems acquisition life cycle.

4.1.3. Systems Engineering Throughout Life-cycle Management

4.1.3. Systems Engineering Throughout Life-cycle Management

A life-cycle approach to system planning, development, and sustainment is fundamental to systems engineering. Related to the total systems approach, DoD Directive 5000.01, E1.1.29 directs the program manager to be accountable for:

Total Systems Approach. The program manager shall be the single point of accountability for accomplishing program objectives for total life cycle systems management, including sustainment. The program manager shall apply human systems integration to optimize total system performance (hardware, software, and human), operational effectiveness and suitability, survivability, safety, and affordability. PMs shall consider supportability, life cycle costs, performance, and schedule comparable in making program decisions. Planning for Operation and Support and the estimation of total ownership costs shall begin as early as possible. Supportability, a key component of performance, shall be considered throughout the system life cycle.

To accomplish life-cycle management, the program manager should consider all systems development decisions in context of the effect that decision will have on the long-term

operational effectiveness, suitability, and affordability of the system. Life-cycle management considerations should permeate the decision making of all acquisition functions and communities, during all acquisition phases. In fact, life-cycle management factors should be considered by the participants in the Joint Capabilities Integration and Development System (JCIDS) activities even before a program manager is assigned; the JCIDS determination of performance capabilities should reflect life-cycle management considerations. Later, under the life-cycle management concept, systems engineering should frame the decision making for sustainment logistics.

Life-cycle management encompasses the following concepts:

- Single point of accountability
- Evolutionary acquisition
- Modifications and upgrades
- Supportability and sustainment as key elements of performance:
    - Performance-based strategies, including logistics
    - Increased reliability, improved maintainability, and reduced logistics footprint
    - Continuing reviews of sustainment strategies.

In executing life-cycle management responsibilities, program managers should apply systems engineering processes and practices known to reduce cost, schedule, and performance risks. This includes best industry practices and technology solutions. The resulting system solution should be interoperable and should meet JCIDS performance capabilities needs. Life-cycle management means that all major materiel alternative considerations and major acquisition functional decisions reflect an understanding of the effects and consequences of these decisions on the Operations and Support phase (including disposal) system effectiveness, suitability, and affordability.

Systems engineering processes are most effective when started early in and applied continuously across the system life cycle. (See section 4.3 for a detailed description of these systems engineering activities by acquisition phase.) The cost to implement a system change increases as a program moves further along the system life cycle. Thus, the greatest flexibility exists in the early stages of development before decisions have been implemented into detailed designs. Early in the life cycle, thorough analyses of life-cycle cost-reduction design practices and cost/performance trade-off studies can result in a balanced design that prevents costly changes later in the life cycle.

Likewise, the Systems Engineering Plan should be established early in the program definition stages and updated periodically as the program matures. Only by starting systems engineering processes early and monitoring them through the life cycle can programs effectively manage cost, schedule, and performance.

4.1.3.1. Systems Engineering Support to Program Formulation

4.1.3.1.1. Early Systems Engineering

Throughout the acquisition process, systems engineering provides the technical foundation for the acquisition program. Particularly in the early stages of an acquisition, systems engineering analysis and products are vital to the early program office's ability to assess appropriately the feasibility of addressing user needs, technology needs of potential solutions, and robust estimates of cost schedule and risk, all leading to predictable, disciplined acquisition. With the increased emphasis in the new DoD Instruction 5000.02 on Materiel Solution Analysis and Technology Development, there is the need for increased emphasis on systems engineering during these phases. A white paper discussing these issues can be accessed at the AT&L (SE) web site.

4.1.3.1.2. Program Formulation during Material Solution Analysis Phase

The Material Solution Analysis Phase identifies one or more materiel solutions to address user capability gaps based on an Analysis of Alternatives (AoA) conducted by an organization independent from the program management office. During Material Solution Analysis, systems engineering plays a role in two ways.

First, during Material Solution Analysis, initial systems engineering is being done as part of the AoA which is essentially a trade study addressing user needs and solution options. This is the case whether or not there is explicit systems engineering support to the AoA, and the amount of engineering emphasis will vary based on the specifics of the capability gap and the options. Engineering considerations should be a component of the AoA guidance and be addressed in the study plan. Without this, approaches could be selected that include technical risk not recognized in the analysis.

Second, the AoA is done independently from the early program management office and forms the basis for selecting the recommended approach(es) for material solution(s). At the close of the AoA, the program office takes ownership of the approach and conducts additional engineering analysis to support the development of the Technical Development Strategy (TDS), the Test and Evaluation Strategy (TES) and the Systems Engineering Plans (SEP).

It is critical that the program management office systems engineering analysis builds upon the AoA results and provides the program manager with the technical basis for Technology Development phase execution, including the critical technology elements (CTEs) requiring risk-reduction efforts. In particular, during Material Solution Analysis the systems engineering team performs the following activities:

- Confirm Concept of Operations (CONOPS) and develop mission and functional threads with users: Beginning with engineering analysis and system requirements definition, a strong foundation in the user CONOPS and mission threads is vital, and a working relationship with the users is essential to achieve a balance between user requirements

(eventually documented in the Capability Development Document (CDD) at Milestone B) and technical feasibility.

- Develop initial view of system requirements and system design concepts: The systems engineering team begins its engineering analysis which could include conducting trade studies and formulating possible system solutions. The analysis effort develops preliminary system functional and performance requirements and possibly overall design options consideration
- Identify critical technology elements: The program team, as part of its system solutions analysis, conducts a technology maturity assessment of the hardware and software options with a focus on the CTEs.
- Determine external interfaces and interoperability: The team needs to understand the context in which potential systems will be employed (based on CONOPS and mission/ functional threads) and how this context affects the system acquisition, including programmatic and technical interfaces and interdependencies. A systems engineering focus on external interfaces and interoperability facilitates an understanding of end-to-end system performance and its implication to the CDD.
- Identify critical protection issues: It is imperative that critical protection issues be identified in the initial stages of systems engineering so that their impact on possible system solutions and requirements can be addressed early and not compel a system redesign after substantial investment has been made.

Results of the Material Solution Analysis systems engineering analysis provide critical technical information to the program planning effort for the Technology Development phase, particularly in determining the plan for CTE risk reduction, prototyping and competing preliminary designs in terms of how much scope, for what objective, and performed by whom (Industry or Government). This technical planning is an essential element of the TDS, and is in a sense the program's initial acquisition strategy. The technical planning is the basis cost estimation and Program Objective Memorandum inputs are prepared. Technical planning outputs are used in developing the Systems Engineering Plan SEP, TDS, and TES and Requests for Proposals, which are documented at Milestone A.

4.1.3.1.3. Program Formulation during Technology Development Phase

The Technology Development Phase has the objectives of buying down technical risk and developing a sufficient understanding of solution development in order to make sound business decisions on initiating a formal acquisition program. Thus there are two types of activities in Technology Development: technology maturation through risk reduction and competitive prototyping, and initial end-item design through preliminary design (when called for in the Technology Development Strategy). In both cases, systems engineering is key to ensuring these activities provide the technical foundation for program decisions.

The activities in the Technology Development Phase include systems engineering to support technology maturation. A key element of systems engineering during technology development is

to mature the critical technologies (either through critical technology element demonstrations or prototyping) needed for a particular system solution implementation (system design and manufacturing processes). The program management office team is the technical manager, employing Industry, Government laboratories, the Services' Science and Technology communities, or Funded Research and Development Centers/Universities to accomplish specific risk reduction or prototype tasks as described in the Systems Engineering Plan. These tasks were identified in the Technology Development Strategy and spelled out in the Request for Proposals/task orders that were prepared either in the Material Solution Analysis phase or post Milestone A. The program management office team completes an assessment of technology maturation results and their impact on the requirements and specific system solutions.

Technology Development Phase activities also address the engineering to support initial end item design when the technology development phase includes activity up to the preliminary design review. For systems with sufficient implementation uncertainty, development of the required end-item system is initiated during the Technology Development phase and continued through to the point of a defined allocated baseline and preliminary design. The knowledge gained in this initial design activity is used to refine the estimated cost, schedule and performance which can be achieved to meet the user capability needs. This initial design activity includes setting system requirements informed by the Capability Development Document (CDD), doing requirements decomposition, establishing the functional architecture, defining the functional baseline, determining the physical architecture, and allocating functionality and performance to the physical elements thereby defining the allocated baseline (preliminary design). This effort may be performed by multiple contractor design teams depending on the program's acquisition strategy. To support the demonstration of design feasibility, these design activities may be supported with design prototypes.

Engineering Analysis: The primary systems engineering objective is to gain sufficient technical knowledge to develop the program's System Requirements Document (SRD) and to verify that the system solution(s) required technology is sufficiently mature (Technology Readiness Level 6 or higher) before proceeding into an end-item design or Milestone B.

System Requirements Document: The program management office team defines system level functional and performance requirements derived from items such as: Concept of Operations, system-level performance metrics, mission threads/use cases, and usage environment, which are captured in a program's SRD.

Competing Design Efforts: Competing contractors execute their technical approach as contained in the proposed Integrated Master Plan and Integrated Master Schedule or similarly produced plan and schedule products, which were part of the proposal and subsequently placed under contract.

Engineering Oversight: With the award of the end-item design contracts, the program management office team, working as an integrated process team with representation from the functional areas across the program, commences oversight of the performing contractors.

Throughout the Technology Development phase, the program management office team works with the users to ensure that the results of the technical work are considered in development of the CDD. Other program management office Integrated Product Teams are informed by the systems engineering team technical work as well as other programmatic activities requiring a program manager decision or opinion. Throughout Technology Development, technical results, culminating with the preliminary design review, provide robust technical information supporting the key Milestone B documents delivered at Milestone B and forming the basis for the formation of a program of record.

4.1.4. System of Systems (SoS) Engineering

A "Systems Engineering Guide for System of Systems" was developed based on the experiences of active SoS systems engineering practitioners and researchers. A SoS is defined as a set or arrangement of systems that results from independent systems integrated into a larger system that delivers unique capabilities. Both systems and SoS conform to the accepted definition of a system, in that each consists of parts, relationships, and a whole that is greater than the sum of its parts. While a SoS is a system, not all systems are SoS. SoS engineering deals with planning, analyzing, organizing, and integrating the capabilities of a mix of existing and new systems into a SoS capability greater than the sum of the capabilities of the constituent parts. SoS engineering is an activity that spans the entire system's life cycle; from pre-Milestone A through Disposal.

There is increased emphasis on SoS in the Department of Defense today as the department places greater emphasis on capabilities as the focus of force development. SoS are being recognized as a way to realize capabilities, and they have thus gained management and engineering attention. In the Department of Defense today, there are several types of SoS, as evidenced by Table 4.1.4.T1. The Future Combat System is the best-known example of a "directed SoS." Communities of interest are good examples of DoD "collaborative SoS," and the Global Information Grid is the predominant DoD "virtual SoS."

Increasingly, the Department of Defense is facing the challenges of "acknowledged SoS," with both recognition of the capability needs, management, and systems engineering of the SoS, but also continued management and technical autonomy of the systems that contribute to the SoS capability objectives. Examples of this type of SoS are the Missile Defense Agency's Ballistic Missile Defense System, the Air Force's Air Operations Center, and the Navy's Naval Integrated Fires Counter Air capability.

Type	Definition
Virtual	Virtual SoS lack a central management authority and a centrally agreed upon purpose for the SoS. Large-scale behavior emerges—and may be desirable—but this type of SoS should rely upon relatively invisible mechanisms to maintain it.

Collaborative	In collaborative SoS, the component systems interact more or less voluntarily to fulfill agreed upon central purposes. The Internet is a collaborative system. The Internet Engineering Task Force works out standards but has no power to enforce them. The central players collectively decide how to provide or deny service, thereby providing some means of enforcing and maintaining standards.
Acknowledged	Acknowledged SoS have recognized objectives, a designated manager, and resources for the SoS; however, the constituent systems retain their independent ownership, objectives, funding, and development and sustainment approaches. Changes in the systems are based on collaboration between the SoS and the system.
Directed	Directed SoS are those in which the integrated SoS is built and managed to fulfill specific purposes. It is centrally managed during long-term operation to continue to fulfill those purposes as well as any new ones the system owners might wish to address. The component systems maintain an ability to operate independently, but their normal operational mode is subordinated to the central managed purpose.

Table 4.1.4.T1. Types of Systems of Systems

In almost all cases, DoD SoS developments are typically not new-start acquisitions but ensembles of existing and new systems that, when put together, address capability needs. In the case of acknowledged SoS, the SoS is an overlay on existing and new systems, where the systems retain their identity, with management and engineering continuing for the systems concurrently with the SoS. SoS managers and systems engineers do not have full control over the component systems, but rather work collaboratively with the managers and systems engineers of the component systems to leverage and influence systems' developments to address SoS needs.

There are seven core elements that characterize systems engineering for SoS. They are the following:

1. translating SoS capability objectives into SoS requirements,
2. assessing the extent to which these capability objectives are being addressed, and
3. anticipating and assessing the impact of external changes on the SoS and constituent systems.
4. Central to SoS systems engineering is understanding the systems that contribute to the SoS and their relationships then documenting through detailed architectures and

5. developing a design for the SoS that acts as a persistent framework for
6. evaluating new SoS requirements and materiel solution options.
7. Finally, the SoS systems engineer orchestrates enhancements to the SoS, monitoring and integrating changes made in the systems to improve the performance of the SoS.

These elements provide the context for the application of the 16 systems engineering technical and technical management processes that are applied in the acquisition of new systems and that support SoS systems engineering. The "Systems Engineering Guide for System of Systems" describes the core elements of SoS systems engineering, their interrelationships, and how the systems engineering processes are applied to support each element.

Finally, as we gain experience in SoS systems engineering, there are a number of cross-cutting approaches that seem to be well suited to this environment. They are listed below.

- SoS systems engineering needs to address organizational as well as technical issues in making systems engineering trades and decisions.
- SoS systems engineers need to acknowledge the role and relationship between the systems engineering done at the component systems versus the SoS level. In general, the more the SoS systems engineer can leave to the component systems engineers of the individual systems, the better.
- Technical management of the SoS needs to balance the level of participation required on the part of the systems, attending to transparency and trust coupled with focused active participation in areas specifically related to the systems and the SoS.
- SoS design needs to be based on open systems and loose coupling that impinges on the systems as little as possible, providing systems maximum flexibility to address changing needs and technology opportunities for their users.
- SoS design strategy and trades need to begin early and continue throughout the SoS evolution, which is an ongoing process.

System of Systems Engineering Implications for Single System Developers

Although the Department of Defense currently focuses on the acquisition of individual systems, program managers of systems should be aware of the fact that their system will ultimately be deployed as part of a larger SoS, whether or not the SoS is formally recognized as such. It is essential that system-level program managers and systems engineers understand the role their system will play in the delivery of user capabilities as part of the larger SoS, so they can incorporate the demands of the SoS into the system requirements and development process. Particular attention should be paid to the specification and management of external interfaces. Program managers should use the following list of questions to address SoS concerns, capitalize on SoS capability pay-offs, and effectively meet the design and development requirements of current and future SoS:

- SoS context for the system

    - Are there system-of-systems capabilities, behavior, and requirements that my system should address to become part of the existing or planned system-of-systems?
- Design for Integration
    - Am I designing my system so that it can be easily integrated with other systems? Does my system have an adaptable and open architecture to enable future reconfiguration and integration into a system of systems?
- Interfaces
    - Have the system of systems interface requirements been adequately defined and documented in the specification of my system?
    - Has my program developed and documented interface control requirements for external functional and physical interfaces?
    - Has my program identified and established conformance testing or certification mechanisms to assure that standards used by external interfaces conform to the prescribed interface specifications?
    - Has my program verified the external functional interface specifications to ensure that the functional and performance requirements for such interfaces are satisfied?
    - Have I established rigorous interface design and management based on conformance and verification of standards at upper layers as well as at the application, transport, network, physical, media, and datalink communication layers?

A Contrasting Note about Engineering a Family of Systems

A family of systems is a grouping of systems having some common characteristic(s). For example, each system in a family of systems may belong to a domain or product line (e.g., a family of missiles, aircraft, or situation awareness systems). In general, a family of systems is not considered to be a system per se because it does not necessarily create capability beyond the additive sum of the individual capabilities of its member systems. A family of systems lacks the synergy of a SoS. The family of systems does not acquire qualitatively new properties as a result of the grouping. In fact, the member systems may not be connected into a whole.

Additional information is available in the "Systems Engineering Guide for System of Systems."

4.1.5. Systems Engineering Within the Integrated Product and Process Development (IPPD) Framework

The DoD defines IPPD as a management technique that uses multidisciplinary teams, i.e., Integrated Product Teams (IPTs), to optimize design, manufacturing, and supportability processes. The IPPD framework facilitates meeting cost and performance objectives from system concept through production, fielding, operations and support, and disposal. Figure 4.1.5.F1 represents a notional IPT. An IPT is a broad, interdisciplinary body that includes engineers, technical specialists, stakeholders, and business and financial analysts. The IPT is as much a

process as it is a meeting body. (See also Guidebook Section 10.3, Section 11.8, and the IPPD Handbook.

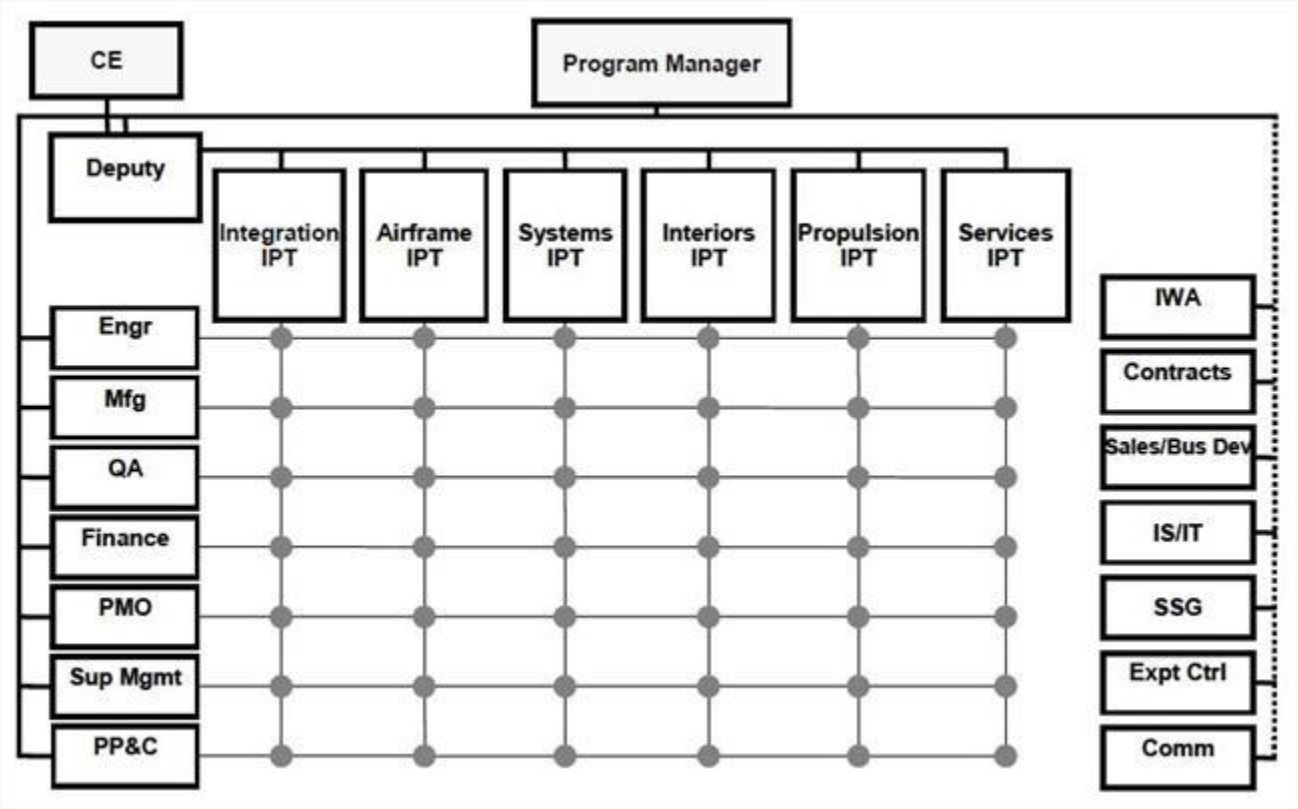


Figure 4.1.5.F1. Notional Integrated Product Team Structure

Systems engineering is consistent with IPPD Handbook and creates and verifies an integrated, life-cycle balanced set of system product and process solutions that satisfy stated customer needs. Systems engineering integrates the development of the system with the development of all system-related processes. The systems engineering processes provide a common basis for and improve the communication between IPT members. All members of the IPTs support systems engineering. Everyone involved in the system's acquisition should consider the total system approach. Each member of the team should apply the systems engineering processes to their respective area of expertise.

Systems engineering participates in the IPPD through a systems engineering working-level IPT (SE WIPT). The program lead or chief engineers should establish an SE WIPT to support the accomplishment of all systems engineering tasks and support efforts. A SE WIPT Charter establishes the participation, roles, authorities, and responsibilities of the SE WIPT. The program manager and chief engineer empowers the SE WIPT and brings the SE WIPT group together often, not only to support milestone and program required documentation but also to support program technical planning, Technical Interchange Meetings (TIMs), technical support to other

WIPTs (e.g., T&E WIPTs), technical reviews, audits, and assessments, and to review program progress and results.

4.1.6. Systems Engineering Leadership

DoD Instruction 5000.02, Enclosure 12, paragraph 3, directs the following:

Each PEO, or equivalent, shall have a lead or chief systems engineer on his or her staff responsible to the PEO for the application of systems engineering across the PEO's portfolio of programs. The PEO lead or chief systems engineer shall:
a. Review assigned programs' SEPs and oversee their implementation
b. Assess the performance of subordinate lead or chief systems engineers assigned to individual programs in conjunction with the PEO and PM.

As part of their overall role in technical oversight of assigned programs, acquisition components should maintain a systems engineering technical authority. Technical authority is the organization outside the program manager's chain of command with responsibility and accountability to establish, approve, and assess conformance of products and technical processes to technical, safety, and certification requirements and policy during all phases of product development, acquisition, and sustainment. This technical authority should ensure not only proper systems engineering process application to programs but also to proper training, qualification and oversight of systems engineering personnel assigned to programs. As part of this overall responsibility for technical oversight, the technical authority should:

- Nominate a lead or chief systems engineer to the program manager at the initial stages of program formulation. The lead or chief systems engineer should be accountable to the program manager for meeting program objectives, and accountable to the systems engineering technical authority for the proper application of systems engineering.
- Nominate a chairperson for each program technical review that is independent of the assigned program team and approved by the program manager, depending on service policy. Technical reviews should include participation by program team personnel and independent (of the program team) subject matter experts as identified by the chair.

4.2. Systems Engineering Processes: How Systems Engineering Is Conducted

This section discusses the use and tailoring of process standards and capability models, presents the program office systems engineering processes as technical management processes and technical processes, and describes common expectations of the systems engineering processes used by contractors (and government Developing Agency or Design Activity).

4.2.1. Process Standards and Capability Models to Accomplish Systems Engineering

Several process standards and capability models describe processes and best practices in accomplishing systems engineering. These standards and capability models usually contain guidance for tailoring, which is best done in conjunction with a risk assessment of the program that leads the program manager to determine which specific processes and activities are vital to the program. Some methods for conducting such an assessment are found in "Understanding and Leveraging a Contractor's CMMI Efforts: A Guidebook for Acquirers." Some recognized systems engineering process standards and capability models include, but are not limited to, the following:

- ISO/IEC 15288, Systems and Software Engineering-System Life Cycle Processes
- ISO/IEC 12207, Systems and Software Engineering -Software Life Cycle Processes
- ISO/IEC 26702, Application and Management of the Systems Engineering Process
- ANSI/EIA 632, Processes for Engineering a System (available for sale)
- CMMI® -DEV, Capability Maturity Model Integration ® for Development
- CMMI®-ACQ, Capability Maturity Model Integration ® for Acquisition

The major distinction between standards and capability maturity models lies in their purpose. Standards provide recommended processes to apply within an organization, describe expected tasks and outcomes, and describe how the processes and tasks integrate to provide required inputs and outputs. Standards are meant to provide an organization with a set of processes that, if done by qualified persons using appropriate tools and methods, will provide a capability to do effective and efficient engineering of systems. Capability maturity models, on the other hand, are for process improvement. Capability maturity models are used to assess, from an organizational perspective, how well the standard processes are being performed. Both capability maturity models and standard processes are useful to an organization, but the role for each should be kept in perspective. To actually accomplish systems engineering, an organization may use any or all of these standards to define and tailor how they will apply systems engineering to their programs. This tailored approach should be coordinated with the systems engineering technical authority for the program. The INCOSE SE Handbook, "A Guide for System Life Cycle Processes and Activities," provides guidance for organizations within the ISO/IEC 15288 framework.

4.2.2. The Contractor's Systems Engineering Processes

4.2.2. The Contractor's Systems Engineering Processes

The solicitation effort should seek descriptions of potential offerors' standards and capability models. Contractor selection should be based on the proposed technical approach, demonstrated domain expertise, and past performance commensurate with the needs of the program supported by demonstrated process capability and organizational maturity in their systems engineering processes.

Organizations use different standards and capability models and their accompanying assessment methods to establish the initial capability of their systems engineering processes and then to improve those processes. When contractors use the Capability Maturity Model Integration (CMMI) models, they often quote a CMMI "level" rating that is the result of an appraisal. DoD does not place significant emphasis on capability level or maturity level ratings, but rather promotes CMMI as a tool for internal process improvement. This lack of emphasis on ratings is prudent in the light of findings that not all suppliers are exhibiting behavior consistent with their attained CMMI maturity level rating. The CMMI models provide a set of best practices to be employed by the supplier and the acquirer. It is essential that DoD and industry use these practices in the right manner and with the appropriate measure. Detailed guidance can be found in "Understanding and Leveraging a Contractor's CMMI Efforts: A Guidebook for Acquirers."

The contractor's Systems Engineering Plan (SEP), Systems Engineering Management Plan (SEMP), or an Offeror's Plan as part of a Proposal in response to a solicitation, is a key tool to assess multiple aspects of any supplier's applied systems engineering approach. This document, if written in response to a government SEP, provides unique insight as to the application of a contractor's standards, capability models, and toolsets to the acquisition program at hand. Additionally, it gives insight as to how the systems engineering technical management and technical processes will be accomplished in the Integrated Product Teams, how systems engineering leadership will be done, and most importantly, how the products of the processes will be developed, assessed, and managed through the systems engineering technical reviews. Best practice is to align the government SEP with the contractor's SEP/SEMP/technical plan following contract award and maintain alignment and currency. Where practical, these documents should initiate a process to unify the program technical planning between government and contractor(s).

4.2.2.1. Capability Reviews

Capability reviews such as manufacturing capability and software capability reviews are a useful tool available during source selections to assess the offerors' capability in selected critical process areas. Capability reviews may be the appropriate means for evaluating program-specific critical processes such as systems engineering, software development, configuration management, etc. The reviews would be useful to supplement process past performance data to ascertain the risks in selecting a given offeror and to assist in establishing the level of government oversight needed to manage the process-associated risks if that offeror is awarded the contract. The trade-off in determining whether or not to do a capability review would be the criticality of the process versus the time and resources to do the review versus the availability, adequacy, and currency of an offeror's process past performance data.

4.2.3. Standardized Process Terminology

The many systems and software engineering process standards and capability models use different terms to describe the processes, activities, and tasks within the systems engineering and

other life-cycle processes. This chapter uses the terminology in Table 4.2.3.T1 to represent generic systems engineering processes. They are grouped in two categories: Technical Management Processes and Technical Processes:

Technical Management Processes	Technical Processes
Decision Analysis	Stakeholders Requirements Definition
Technical Planning	Requirements Analysis
Technical Assessment	Architectural Design
Requirements Management	Implementation
Risk Management	Integration
Configuration Management	Verification
Technical Data Management	Validation
Interface Management	Transition

Table 4.2.3.T1. Chapter Terminology

These generic processes are described briefly below and applied throughout the life-cycle phases. More detail with regard to systems engineering processes can be found in any of the above-mentioned standards or capability models. Because systems engineering cannot be conducted without good organization and project processes, as well as sufficient infrastructure, these standards and capability models also may include processes and activities, such as organizational training, that are beyond the technical ones that may be considered specific to systems engineering. Throughout this chapter, the term "system element" is used to indicate a subsystem, a component, or a configuration item, depending on the systems engineering context and phase of acquisition under discussion. Also, throughout this document, the term "configuration item" generally refers to both software and hardware items.

4.2.3.1. Technical Management Processes

The program manager uses technical management processes to manage the technical development of the system increments, including the supporting or enabling systems. This section of the Guidebook discusses the eight technical management processes that are used throughout the life cycle. Section 4.2.5 describes the eight technical processes. Section 4.5 describes in detail the key techniques and tools for technical management, oversight and analysis.

4.2.3.1.1. Decision Analysis

Decision Analysis is a discipline that employs many procedures, methods, and tools for identifying, representing, and formally assessing the important aspects of alternative decisions (options) to select an optimum (i.e., the best possible) decision. Decision Analysis activities provide the basis for evaluating alternatives and selecting the optimum decision. It involves selecting the criteria for the decision and the methods to be used in conducting the analysis. For example, during system design, analysis is conducted to help chose among alternatives to achieve a balanced, supportable, safe, robust, and cost-effective system design. These analyses include, but are not limited to, trade studies, system analysis, system safety analyses, trade off analysis, supportability analysis, level of repair analysis, post fielding support analysis, repair versus discard analysis, and cost analysis. These studies/analyses should be augmented with models and simulation, or virtual and/or physical prototypes, where applicable, before making decisions on the best alternative. The criteria to determine the best alternative may include, for example, interoperability constraints, size, transportability requirements, maintenance concept, producibility, affordability, reliability, availability and maintainability goals, and schedule.

The Decision Analysis process for system of systems includes the development of integrated approaches that rely on data sharing, collaboration, and interoperability to execute assessment and decision making effectively. The system of systems analysis plan should consider the constituent systems analysis plans and integrate such plans across multiple organizations.

4.2.3.1.2. Technical Planning

Technical Planning activities provide the critical quantitative input to program planning and ensure that the systems engineering processes are applied properly throughout a system's life cycle. Technical Planning defines the scope of the technical effort required to develop, field, and sustain the system.The scope of the technical effort includes the following:

1. Work Breakdown Structure for the technical activities and tasks,
2. Integrated Master Plan for all technical activities and tasks,
3. Time phased sequence of the technical effort in an event driven Integrated Master Schedule, and
4. Resources (skilled workforce, support equipment/tools and facilities) required to develop, field, and sustain the system.

The scope of the technical effort is critical to provide the basis for a program cost estimate (Independent Cost Estimate and/or Cost Analysis Requirements Document), Risk Identification and Risk Analysis, and to provide the quantitative measures supporting the Technical Assessment Process. Also, the resulting program estimates and risk assessments are essential elements to support Milestone Review decisions, establish the Performance Measurement Baseline and enable mandatory program certifications (e.g., section 2366a or section 2366b).

A mandated tool for Technical Planning, required for every program milestone, is the Systems Engineering Plan. Each of the 16 technical and technical management processes requires

planning. The application of these technical processes can identify constraints, dependencies, and interfaces that will result in derived technical requirements.

4.2.3.1.3. Technical Assessment

Technical Assessment activities measure technical progress and assess both program plans and requirements. Activities within Technical Assessment include those associated with Technical Performance Measurement, the conduct of Technical Reviews (including Preliminary Design Review/Critical Design Review Reports), Program Management Review (PMR), Technical Interchange Meeting (TIM), Interface Control Working Group (ICWG), Program Support Reviews (PSR), Assessment of Operational Test Readiness (AOTR), Risk Identification, the support of Certification (System or Program), and Earned Value Management (EVM) (whenever it is required in accordance with DoD Instruction 5000.02, Table 5, EVM Implementation Policy). A structured technical review process should demonstrate and confirm completion of required accomplishments and exit criteria as defined in program and system planning. The Preliminary Design Review is an example of a technical review that is mandatory for all MDAPs and will be scheduled before MS B. Technical reviews are discussed in detail in Section 4.3 and summarized in Section 4.5.9. Technical Assessment activities discover problems (deficiencies or anomalies) and warnings of potential program problems that often lead to corrective action. This information is provided to the Program Manager and contributes to the Quarterly Defense Acquisition Executive Summary (DAES) Report.

A TIM is often held to address technical issues and will result in detailed discussion of technical alternatives, risks, recommendations, and action items. The government and industry team members attend the technical meeting as required to address the agenda and meeting purpose. Typically, the Statement of Work (SOW) tasks the contractor to participate in the TIM, capture minutes, and forward any TIM findings or any recommendations to the responsible Integrated Product Team(s) (IPT) or lead systems engineer.

A PMR is regularly conducted at defined intervals (monthly or quarterly) by the Program Manager for the purpose of determining the status of an assigned system. PMRs are designed as tools to report program status, identify issues and problems, discuss risks, and to develop appropriate follow-up actions as required. Typically, the SOW tasks the contractor to participate in the PMR and to capture minutes.

The ICWG is the traditional forum to establish official communications links between those responsible for the design of interfacing systems or components. Within the IPT framework, ICWGs can be integrated teams that establish linkages between interfacing design IPTs, or could be integrated into a system-level engineering working group. Membership of ICWGs or comparable integrated teams should include representatives from each contractor, significant vendors, and participating government agencies the procuring program office (external and selected top-level interfaces) or prime contractor (internal interfaces) generally designates the chair.

The Director of Systems Engineering shall have access to any DoD component records or data relating to systems engineering and development planning (including classified, unclassified, competition sensitive, and proprietary information) necessary to carry out assigned duties (see Directive-Type Memorandum (DTM) 09-027 – Implementation of the Weapon Systems Acquisition Reform Act of 2009).

4.2.3.1.4. Requirements Management

Requirements Management provides traceability back to user-defined capabilities as documented through either the Joint Capabilities Integration and Development System or other user-defined source, and to other sources of requirements. Requirements traceability is one function of requirements management. As the systems engineering process proceeds, requirements are developed to increasing lower levels of the design. Requirements traceability is conducted throughout the system life cycle and confirmed at each technical review. Traceability between requirements documents and other related technical planning documents, such as the Test and Evaluation Master Plan, should be maintained through a relational data base, numbering standards, or other methods that show relationships. A good requirements management system should allow for traceability from the lowest level component all the way back to the user capability document or other source document from which it was derived. The program manager should institute Requirements Management to do the following:

- Maintain the traceability of all requirements from capabilities needs through design and test,
- Document all changes to those requirements, and
- Record the rationale for those changes.

Emerging technologies and threats can influence the requirements in the current as well as future increments of the system. In evolutionary acquisition and systems of systems, the management of requirements definition and changes to requirements take on an added dimension of complexity.

4.2.3.1.5. Risk Management

Risk management is the overarching process that encompasses identification, analysis, mitigation planning, mitigation plan implementation, and tracking. Risk management should begin at the earliest stages of program planning and continue throughout the total life cycle of the program. Additionally, risk management is effective only if it is fully integrated with the program's systems engineering and program management processes. This is accomplished through the identification of risk drivers, dependencies, root causes, and consequence management. A common misconception, and program office practice, concerning risk management is to identify and track issues (vice risks) and then manage the consequences (vice the root causes). Risks should not be confused with issues (realized risks). If a root cause is described in the past tense,

the root cause has already occurred, and is therefore an issue that needs to be resolved but not a risk.

Risk management is critical to acquisition program success. Addressing risk on programs helps ensure that program cost, schedule, and performance objectives are achieved at every stage in the life cycle and communicates to stakeholders the process for uncovering, determining the scope of, and managing program uncertainties. Because risk can be associated with all aspects of a program, it is important to recognize that risk identification is part of everyone's job, not just that of the systems engineer or program manager.

Risk

- Risk is a measure of future uncertainties in achieving program performance goals and objectives within defined cost, schedule, and performance constraints. Risk can be associated with all aspects of a program (e.g., threat environment, hardware, software, human interface, technology maturity, supplier capability, design maturation, performance against plan,) as these aspects relate across the work breakdown structure and Integrated Master Schedule.
- The impact of software development and integration efforts should be addressed as part of the program's risk management activities. Risk addresses the potential variation in the planned approach and its expected outcome.

Risk has three components:

- A future root cause (yet to happen), which, if eliminated or corrected, would prevent a potential consequence from occurring,
- A probability (or likelihood) assessed at present of that future root cause occurring, and
- The consequence (or effect) of that future occurrence.

A future root cause is the most basic reason for the presence of a risk. Accordingly, risks should be linked to future root causes and their effects.

The risk management process includes the following key activities, performed on a continuous basis (See Figure 4.2.3.1.5.F1 Risk Management Process – Key Activities):

- Risk Identification
- Risk Analysis,
- Risk Mitigation Planning,
- Risk Mitigation Plan Implementation, and
- Risk Tracking.

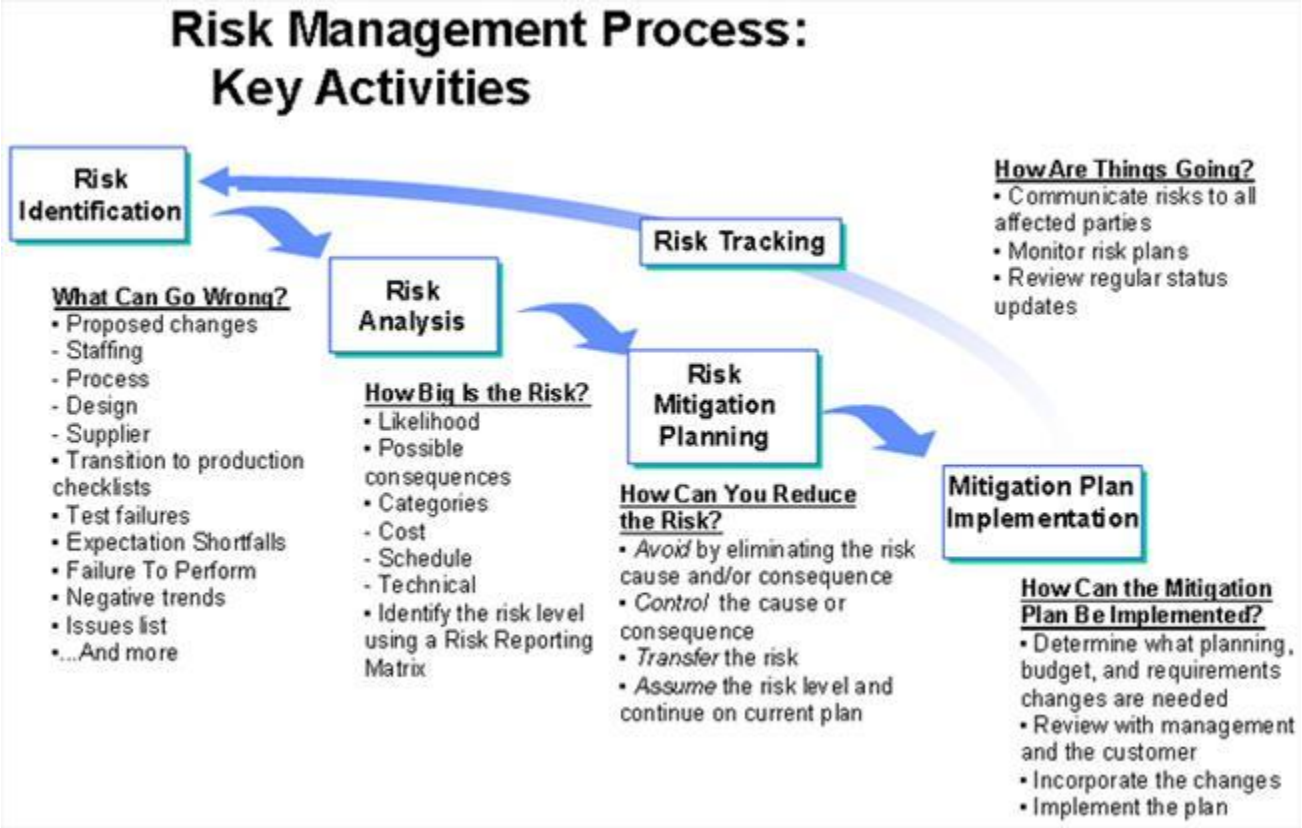


Figure 4.2.3.1.5.F1. Risk Management Process – Key Activities

Risk Identification

Risk identification is the activity that examines each element of the program to identify associated root causes, begin their documentation, and set the stage for their successful management. Risk identification begins as early as possible in successful programs and continues throughout the program with regular reviews and analyses of Technical Performance Measurements/Critical Technical Parameters, schedule, resource data, life-cycle cost information, Earned Value Management data/trends, progress against critical path, technical baseline maturity, safety, operational readiness, and other program information available to program Integrated Product Team members.

The intent of risk identification is to answer the question "What can go wrong?" by:

- Looking at current and proposed staffing, process, design, supplier, operational employment, resources, dependencies, etc.,
- Monitoring test results especially test failures (readiness results and readiness problems for the sustainment phase),
- Reviewing potential shortfalls against expectations,

- Analyzing negative trends, and
- Conducting system safety and environmental analyses.

Risk Analysis

The intent of risk analysis is to answer the question "How big is the risk?" by:

- Considering the likelihood of the root cause occurrence;
- Identifying the possible consequences in terms of performance, schedule, and cost; and
- Identifying the risk level using the Risk Reporting Matrix.

Each undesirable event that might affect the success of the program (performance, schedule, and cost) should be identified and assessed as to the likelihood and consequence of occurrence. A standard format for evaluation and reporting of program risk assessment findings facilitates common understanding of program risks at all levels of management. The Risk Reporting Matrix below is typically used to determine the level of risks identified within a program. The level of risk for each root cause is reported as low (green), moderate (yellow), or high (red).

Risk Mitigation Planning

The intent of risk mitigation planning is to answer the question "What is the program approach for addressing this potential unfavorable consequence?" One or more of these mitigation options may apply:

- Avoiding risk by eliminating the root cause and/or the consequence,
- Controlling the cause or consequence,
- Transferring the risk, and/or
- Assuming the level of risk and continuing on the current program plan.

Risk mitigation planning is the activity that identifies, evaluates, and selects options to set risk at acceptable levels given program constraints and objectives. Risk mitigation planning is intended to enable program success. It includes the specifics of what should be done, when it should be accomplished, who is responsible, and the funding and schedule tasks required to implement the risk mitigation plan. The most appropriate program approach is selected from the mitigation options listed above and documented in a risk mitigation plan. The level of detail depends on the program life-cycle phase and the nature of the need to be addressed. However, there must be enough detail to allow a general estimate of the effort required and technological capabilities needed based on system complexity.

Risk Mitigation Plan Implementation

The intent of risk mitigation (plan) execution is to ensure successful risk mitigation occurs. It answers the question "How can the planned risk mitigation be implemented?"

It:

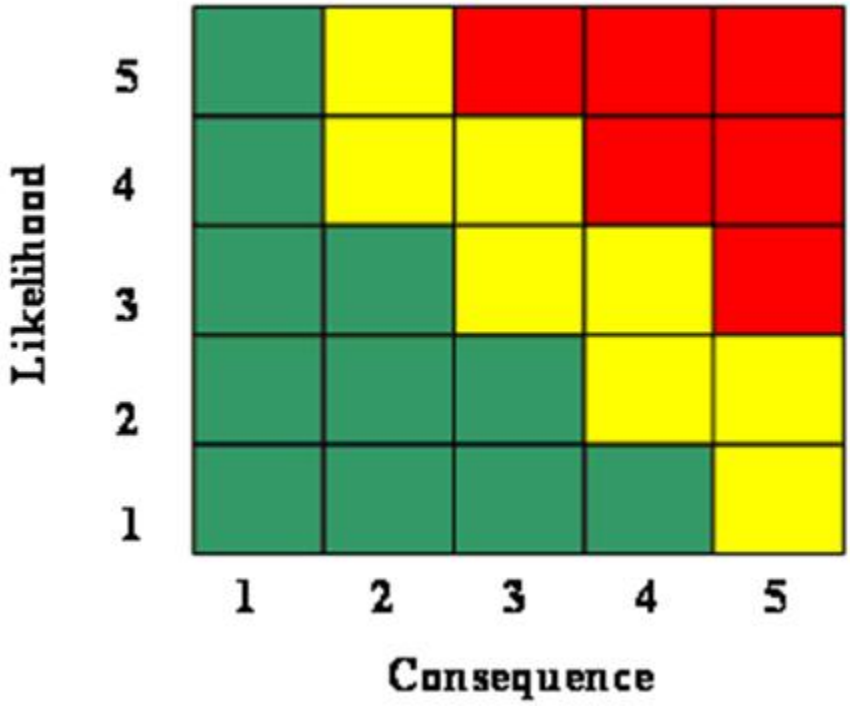
- Determines what planning, budget, schedule tasks, requirements and contractual changes are needed,
- Provides a coordination vehicle with management and other stakeholders,
- Directs the teams to execute the defined and approved risk mitigation plans,
- Outlines the risk reporting requirements for on-going monitoring, and
- Documents the change history.

Implementing risk mitigation should also be accomplished by risk category, and it is important for this process to be worked through the IPT structure, requiring the IPTs at each WBS level to scrub and endorse the risk mitigations of lower levels. It is important to mitigate risk where possible before passing it up to the next WBS level. In addition, each IPT must communicate potential cost or schedule growth to all levels of management. It is imperative that the Systems Engineer and Program Manager understand and approve the mitigation plan and examine the plan in terms of secondary, unforeseen impacts to other elements of the program outside of the risk owning IPT. As part of this effort, the IPTs should ensure effective mitigation plans are implemented and ongoing results of the risk management process are formally documented and briefed, as appropriate, during program and technical reviews.

Risk Tracking

The intent of risk tracking is to ensure successful risk mitigation. It answers the question "How are things going?" by:

- Communicating risks to all affected stakeholders,
- Monitoring risk mitigation plans,
- Reviewing regular status updates,
- Displaying risk management dynamics by tracking risk status within the Risk Reporting Matrix (see Figure 4.2.3.1.5. F2), and,
- Alerting management as to when risk mitigation plans should be implemented or adjusted.



Risk tracking activities are integral to good program management. At a top level, periodic program management reviews and technical reviews provide much of the information used to identify any performance, schedule, readiness, and cost barriers to meeting program objectives and milestones. Risk tracking documents may include: program metrics, technical reports, earned value reports, watch lists, schedule performance reports, technical review minutes/reports, and critical risk processes reports.

Typical risk sources include:

- Threat. The sensitivity of the program to uncertainty in the threat description, the degree to which the system design would have to change if the threat's parameters change, or the vulnerability of the program to foreign intelligence collection efforts (sensitivity to threat countermeasure).
- Requirements. The sensitivity of the program to uncertainty in the system description and requirements, excluding those caused by threat uncertainty. Requirements include operational needs, attributes, performance and readiness parameters (including KPPs), constraints, technology, design processes, and WBS elements.
- Technical Baseline. The ability of the system configuration to achieve the program's engineering objectives based on the available technology, design tools, design maturity, etc. Program uncertainties and the processes associated with the "ilities" (reliability, supportability, maintainability, etc.) must be considered. The system configuration is an agreed-to description (an approved and released document or a set of documents) of the attributes of a product, at a point in time, which serves as a basis for defining change.

- Test and Evaluation. The adequacy and capability of the test and evaluation program to assess attainment of significant performance specifications and determine whether the system is operationally effective, operationally suitable, and interoperable.
- Modeling and Simulation (M&S). The adequacy and capability of M&S to support all life-cycle phases of a program using verified, validated, and accredited models and simulations.
- Technology. The degree to which the technology proposed for the program has demonstrated sufficient maturity to be realistically capable of meeting all of the program's objectives.
- Logistics. The ability of the system configuration and associated documentation to achieve the program's logistics objectives based on the system design, maintenance concept, support system design, and availability of support data and resources.
- Production/Facilities. The ability of the system configuration to achieve the program's production objectives based on the system design, manufacturing processes chosen, and availability of manufacturing resources (repair resources in the sustainment phase).
- Concurrency. The sensitivity of the program to uncertainty resulting from the combining or overlapping of life-cycle phases or activities.
- Industrial Capabilities. The abilities, experience, resources, and knowledge of the contractors to design, develop, manufacture, and support the system.
- Cost. The ability of the system to achieve the program's life-cycle support objectives. This includes the effects of budget and affordability decisions and the effects of inherent errors in the cost estimating technique(s) used (given that the technical requirements were properly defined and taking into account known and unknown program information).
- Management. The degree to which program plans and strategies exist and are realistic and consistent. The government’s acquisition and support team should be qualified and sufficiently staffed to manage the program.
- Schedule. The sufficiency of the time allocated for performing the defined acquisition tasks. This factor includes the effects of programmatic schedule decisions, the inherent errors in schedule estimating, and external physical constraints.
- External Factors. The availability of government resources external to the program office that are required to support the program such as facilities, resources, personnel, government furnished equipment, etc.
- Budget. The sensitivity of the program to budget variations and reductions and the resultant program turbulence.
- Earned Value Management System. The adequacy of the contractor’s EVM process and the realism of the integrated baseline for managing the program.

Risk Management Tools:

There are many types of software solutions available to help you with risk management tasks. Each tool provides some specific capability as part of an overall Risk Management process. The Tools can largely be broken down into the following categories:

- Risk Management Systems - web-based, highly scalable systems (running on databases such as MS SQL Server or Oracle) that integrate into planning or requirements applications (such as Telelogic DOORS, MS Project or Primavera) and assist with the identification, assessment, management, analysis, reporting and communication of risk information (cost, schedule, technical, etc.) on projects and operations.
- Standalone Tools - may be web-based or client tools that are limited in scalability (normally running on databases such as Excel or Access) that assist with some or all of the following on smaller projects: identification, assessment, analysis, and communication of risk information.
- Analysis Tools - assist in the quantification of risk information (normally one or more of the following: cost, schedule and/or technical) from either a risk register or a planning applications (such as Microsoft Project or Primavera).

Additional information on this subject is in the Risk Management Guide for DoD Acquisition and the MIL-STD-882D, "DoD Standard Practice for System Safety" for environment, safety, and occupational health risk management (see section 4.4.7.5).

4.2.3.1.6. Configuration Management

4.2.3.1.6. Configuration Management

DoD Instruction 5000.02, Enclosure 12, paragraph 5, directs the use of configuration management across the total system life cycle per the following extract:

The PM shall use a configuration management approach to establish and control product attributes and the technical baseline across the total system life cycle. This approach shall identify, document, audit, and control the functional and physical characteristics of the system design; track any changes; provide an audit trail of program design decisions and design modifications; and be integrated with the SEP and technical planning. At completion of the system level Critical Design Review, the PM shall assume control of the initial product baseline for all Class 1 configuration changes.

Configuration management is the application of sound program practices to establish and maintain consistency of a product's or system's attributes with its requirements and evolving technical baseline over its life. It involves interaction among government and contractor program functions such as systems engineering, hardware/software engineering, specialty engineering, logistics, contracting, and production in an Integrated Product Team environment. The program manager should use configuration management to establish and mature the technical baseline throughout the acquisition life cycle.

4.2.3.1.6.1. Configuration Management of the Technical Baseline

The technical baseline includes user requirements, program and product information and related documentation for all configuration items (i.e., those system elements under configuration management). Configuration items can consist of the integrated master schedule, system requirements, specifications, hardware, software, and documentation (data). A configuration management process guides the system products, processes, and related documentation, and facilitates the development of open systems. Configuration management efforts result in a complete audit trail of plans, decisions and design modifications. Configuration management functions include the following:

- Planning and Management—Provides total life-cycle configuration management planning for the program/project and manages the implementation of that planning,
- Identification—Establishes configuration information and documentation of functional and physical characteristics of each configuration items. Documents agreed-to configuration baselines and changes to those configurations that occur over time,
- Change Management—Ensures that changes to a configuration baseline are properly identified, recorded, evaluated, approved or disapproved, and incorporated and verified, as appropriate. A common change method is the Engineering Change Proposal. See MIL-HDBK-61A.
- Status Accounting—Manages the capture and maintenance of product configuration information necessary to account for the configuration of a product throughout the product life cycle, and
- Verification and Audit—Establishes that the performance and functional requirements defined in the technical baseline are achieved by the design and that the design is accurately documented in the technical baseline.

The technical baseline consists of many configuration documents, technical review artifacts, and information objects. Typically these include: specifications, drawings, interface control documents, requirements, parts lists or bill of materials, software documentation, standards, processes, models and simulations, architecture descriptions, and other associated items. A technical data package is the subset of this information associated with a related acquisition, production, engineering, or sustainment activity.

4.2.3.1.6.2. Establishment of Configuration Baselines

The concept of baselines is central but not unique to configuration management. The Acquisition Program Baseline (APB) provides key cost, schedule, and performance objectives and thresholds for each major program milestone. Similarly, configuration baselines are established for specific events and contribute to the performance portion of a program's APB. Typically, a configuration baseline would be established for each of the technical reviews discussed throughout Section 4.3 and summarized in Section 4.5.9.

At a minimum, to mature the technical baseline, the following configuration baselines should be established:

- Functional Baseline—Definition of the required system functionality describing functional and interface characteristics of the overall system, and the verification required to demonstrate the achievement of those specified functional characteristics. This baseline is derived from the Capability Development Document (CDD) and normally includes a detailed functional performance specification for the overall system and the tests necessary to verify and validate overall system performance. The functional baseline is normally established and put under configuration control at the System Functional Review. It is usually verified with a System Verification Review and/or a Functional Configuration Audit (FCA).
- Allocated Baseline—Definition of the configuration items making up a system, and then how system function and performance requirements are allocated across lower level configuration items (hence the term allocated baseline). It includes all functional and interface characteristics that are allocated from the top level system or higher-level configuration items, derived requirements, interface requirements with other configuration items, design constraints, and the verification required to demonstrate the traceability and achievement of specified functional, performance, and interface characteristics. The performance of each configuration item in the allocated baseline is described in its preliminary design specification as are the tests necessary to verify and validate configuration item performance. The allocated baseline is usually established and put under configuration control at each configuration item's (hardware and software) Preliminary Design Review (PDR), culminating in a system allocated baseline established at the system-level PDR.
- Product Baseline—Documentation describing all of the necessary functional and physical characteristics of a configuration item; the selected functional and physical characteristics designated for production acceptance testing; and tests necessary for deployment/installation, operation, support, training, and disposal of the configuration item. The initial product baseline includes "build-to" specifications for hardware (product, process, material specifications, engineering drawings, and other related data) and software (software module design— "code-to" specifications). The Initial product baseline is usually established and put under configuration control at each configuration item's Critical Design Review (CDR), culminating in an initial system product baseline established at the system-level CDR. By DoD policy, the PM shall assume control over this initial product baseline after the system-level CDR and control all Class 1 changes. Until completion of the System Verification Review (SVR) and/or FCA, Class 1 changes shall be those changes that affect the government performance specification. Following the SVR/FCA, the government will further define contractually what constitutes a Class 1 change. The system product baseline is finalized and validated at the Physical Configuration Audit.

Figure 4.2.3.1.6.2.F1 shows the relationship of the various configuration baselines and a specification tree for a sample program.

Once established, these configuration baselines (functional, allocated, product) may be managed by either the program office or the contractor, depending upon the nature of the contractual relationship between the parties. Additional information on configuration management processes is provided in the following standards and best practices:

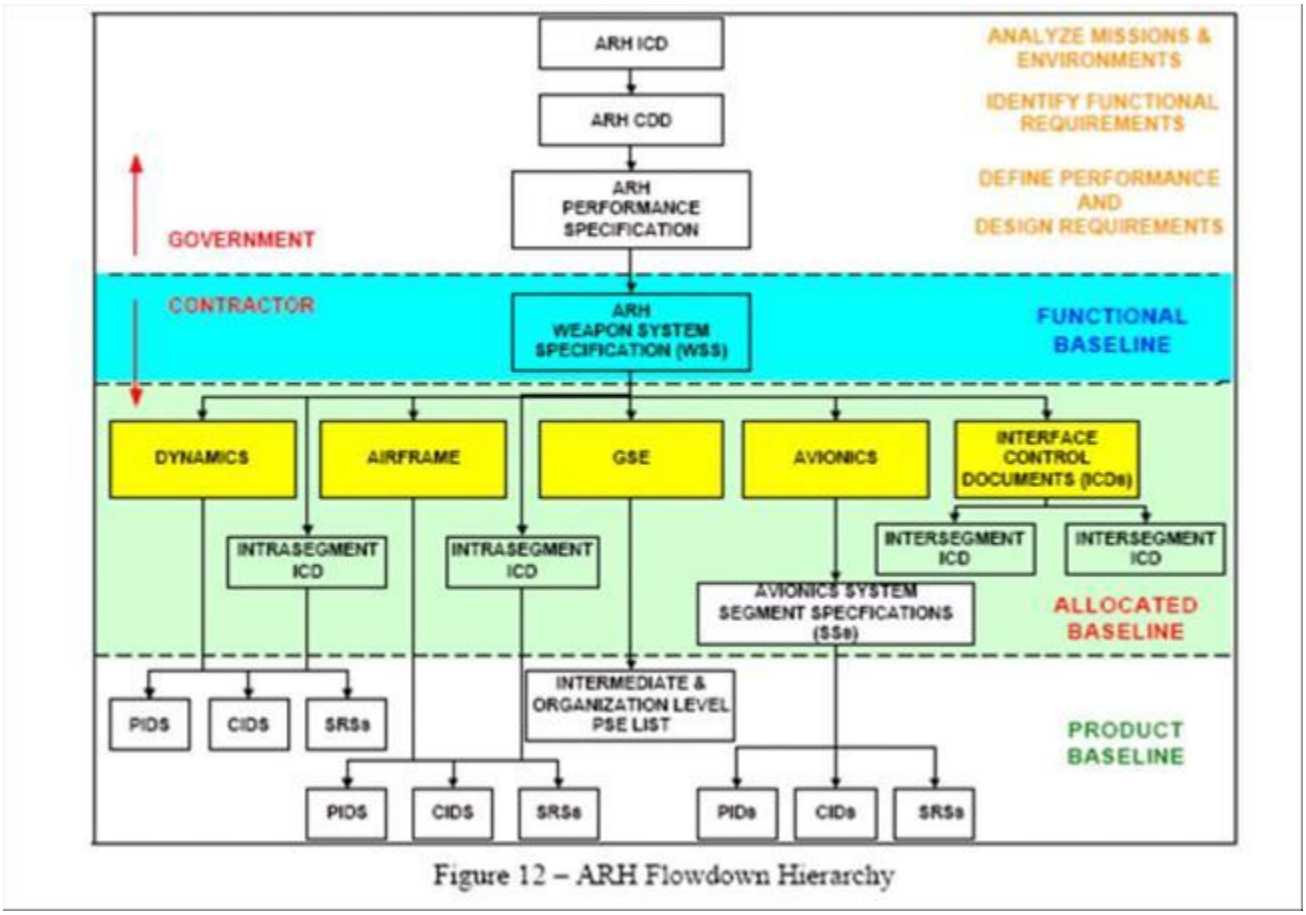


Figure 4.2.3.1.6.2.F1. Depiction of a sample set of configuration baselines

- ANSI/EIA 649A, "Configuration Management," available for sale on the Information Technology Association of America website
- ISO 10007, "Quality management systems - Guidelines for configuration management," available for sale on the American National Standards Institute website
- ISO/TS 10303-403:2008, "Industrial automation systems and integration - Product data representation and exchange - Part 403: Application module: AP203 configuration controlled 3D design of mechanical parts and assemblies," available for sale on the American National Standards Institute website
- EIA-836-A, "Configuration Management Data Exchange and Interoperability," available for sale on the Information Technology Association of America website
- MIL-HDBK-61A, "Configuration Management Guidance"
- MIL-STD-1916, "DOD Preferred Methods for Acceptance of Product"

4.2.3.1.7. Data Management

4.2.3.1.7. Data Management

Data are defined as recorded information regardless of the form or method of recording. Data management applies policies, procedures and information technology to plan for, acquire, access, manage, protect, and use data of a technical nature to support the total life cycle of the system. Data is used to gain insight and provide guidance to systems development programs through sustainment.

Data management in this chapter will focus on technical data, which is any data other than computer software that is of a scientific or technical nature. This includes data associated with system development, configuration management, test and evaluation, installation, parts, spares, repairs and product sustainment. Data specifically not included would be data relating to tactical operations information; sensor or communications information; financial transactions; personnel data; and other data of a purely business nature. Technical data can exist in many forms: paper or electronic documents, specifications, drawings, lists, records, repositories, standards, models, correspondence, and other descriptions of a system. Additional guidance relative to data is contained in section 5.1.6.

Data management plays an important role in facilitating other systems engineering processes. Data management:

- Enables collaboration and life cycle use of acquisition system product data,
- Captures and organizes all systems engineering artifacts input to, processed by, or output from systems engineering processes,
- Documents traceability among requirements, designs, solutions, decisions, and rationale,
- Records engineering decisions, procedures, methods, results, and analyses,
- Facilitates technology insertion for affordability improvements during reprocurement and post-production support,

- Supports configuration management, risk management, interface management, requirements management, trade-off analyses, technical assessment, and technical review activities, and
- Enables advanced concepts based on Integrated Digital Environments, such as Knowledge-Based Acquisition, and model based systems engineering (also see section 11.13).

Data management also enables sharing of system data that is required to support collaboration and oversight with other government and industry organizations and authorities.

Under the life cycle management approach, the program manager is responsible for data management for each phase of the system life cycle. The program manager should determine the data needs of the program (including external obligations) and develop a long-term strategy that integrates data requirements across all functional disciplines. Corresponding plans for data management should be included in the Systems Engineering Plan. This responsibility includes proper indexing and management of product data, to include indexing that data within the Military Engineering and Data Asset Locator System (MEDALS), to formally store that data for the life cycle of the program, and beyond. The following resources provide additional information related to data management:

- Data Management Community of Practice (CoP), located on the Acquisition Community Connection on the Defense Acquisition University (DAU) website,
- DoD 5010.12-M, Procedures for the Acquisition and Management of Technical Data, May 1993 (http://www.dtic.mil/whs/directives/corres/html/501012m.htm),
- GEIA-859, Consensus Standard for Data Management, located on the GEIA website (http://www.geia.org/) (click on STANDARDS), and
- "Intellectual Property: Navigating Through Commercial Waters", October 15, 2001.

4.2.3.1.7.1. Data Acquisition

Data acquisition encompasses all activities that create, obtain, or access data from internal or external sources to satisfy data requirements driven by the data strategy. When at all possible, data should be acquired in a structured format that is independent of the method of access or delivery and defined by or based on open standards. Open data exchange formats promote interoperability of systems engineering tools and repositories, improve the meaning and understanding of data and its reuse, foster collaboration and competition, and help to ensure access to data consistently throughout the system life cycle and across systems of systems. Consider the following standards for defining the structure of digital data:

- ISO 10303, Standard for the Exchange of Product Model Data STEP),
- Object Management Group (OMG) Systems Modeling Language (SysML), (http://www.omgsysml.org/)
- S1000D International Specification for Technical Publications Utilizing a Common Source Database (http://www.s1000d.org/)

- The decision to purchase data should be carefully examined, as there may be situations where access to required data is not sufficient to support life cycle needs. DoD 5010.12-M provides information specific to acquiring data from contractors, such as the role and use of Contract Data Requirements Lists and Data Item Descriptions. PMs should always consult with contracting and legal subject matter experts when crafting technical data acquisition strategies.

4.2.3.1.7.2. Data Protection

The program manager is responsible for protecting system data, whether the data is stored and managed by the government or by contractors. The DoD policy with regard to data protection, marking, and release can be found in DoD Directive 5230.24, DoD Directive 5230.25, DoD 5400.7-R, and DoD 5200.1-M. Data containing information subject to restrictions are required to be protected in accordance with the appropriate guidance, contract, or agreement. Guidance on distribution statements, restrictive markings, and restrictions on use, release, or disclosure, of data can be found in the DFARS Part 252.227-7013 &7014, and DoD Directive 5230.24. When digital data is used, the data should display applicable restriction markings, legends, and distribution statements clearly visible when the data is first opened or accessed. These safeguards not only assure government compliance with use of data but also guarantee and safeguard contractor data that are delivered to the government, and extend responsibilities of data handling and use to parties who subsequently use the data.

Section 208 of Public Law 107-347 and DoD Privacy Impact Assessment (PIA) guidance requires that PIA be conducted prior to developing or purchasing any DoD information system that will collect, maintain, use, or disseminate personally identifiable information about members of the public, federal personnel, DoD contractors and, in some cases, foreign nationals. Available PIA Guidance provides procedures for completing and approving PIAs in the Department of Defense. For further details, see section 7.5.6.4.

All data deliverables should include distribution statements. Processes should be established to protect all data that contain critical technology information, as well as ensure that limited distribution data, intellectual property data, or proprietary data is properly handled throughout the life cycle, whether the data are in hard-copy or digital format.

4.2.3.1.7.3. Data Storage

The program manager also has responsibility for addressing long-term storage and retrieval of data and associated program information. This includes long-term planning and incremental digitization, as required, to ensure that applicable data are available, preserved, and migrated to successive formats for future planning and use.

4.2.3.1.7.4. Definition and Scope of Data

The topic of data is very broad and relevant to all stakeholders in an enterprise or project that produce, consume and manage data. The DFARS provides specific definitions for data, and it is important to understand the context and associated definitions when engaging in data related discussions. The figure below depicts a hierarchy of the types of data that are relevant to an enterprise or project. Each data element, tagged 1, 2 and 3, are followed with definitions.

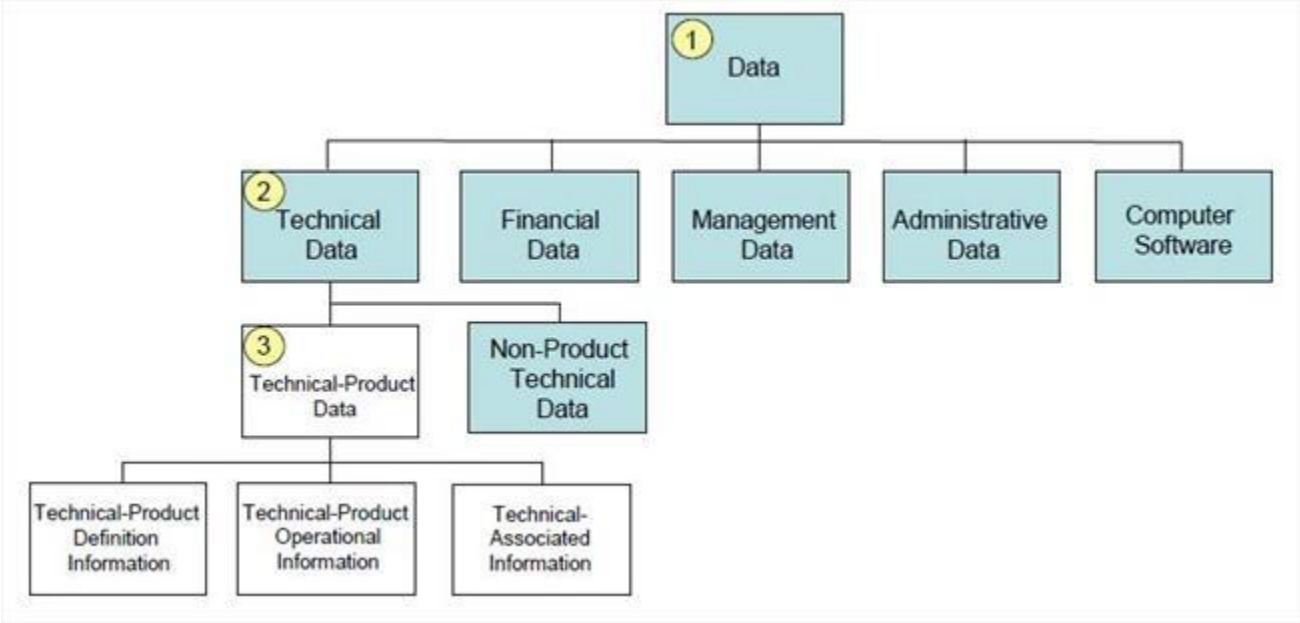


Figure 4.2.3.1.7.4.F. Data Depiction and Scope

4.2.3.1.7.4.1. Data Definition (1)

The term Data is the broadest definition of data and applies to the entire project or enterprise. Data is defined as follows:

"Recorded information regardless of the form or method of recording. The term includes technical data, computer software documentation, financial information, management information, representation of facts, numbers, or datum of any nature that can be communicated, stored, and processes to form information and other information required by a contract to be delivered to, or accessed by, the Government." DFARS

4.2.3.1.7.4.2. Technical Data Definition (2)

For the purposes of DoD acquisition programs and the acquisition and management of data; technical data is the scope of interest. The term technical data is defined as:

"Recorded information (regardless of the form or method of the recording) of a scientific or technical nature (including computer software documentation) relating to supplies procured by an agency. Such term does not include computer software or financial, administrative, cost or pricing, or management data or other information incidental to contract administration." See 10 U.S.C. 2302(4)."

For ACAT I and II programs, a Data Management Strategy (DMS) is required prior to each milestone review as part of the Acquisition Strategy. The acquisition, management, and rights are defined in the DMS. For additional guidance regarding the DMS, refer to Guidebook sections 2.2.14 and 5.1.6.4.

4.2.3.1.7.4.3. Technical-Product Data Definition (3)

The term Technical Product data defines the data that systems engineering have primary concern. Systems engineering is a key stakeholder in the development of the DMS and should advocate the technical product data that needs to be included in the DMS. The definition of Technical Product Data is:

"Information that describes the product's performance, functional, and physical attributes, including requirements information (e.g. specifications and requirements documents) and design information (e.g. drawings, part models, software listings and design descriptions). Product information provides the technical basis for actions taken during all product life-cycle phases for product validation and for product operational information."

Technical-Product Data is "All data created as a consequence of defining (requirements), designing, testing, producing, packaging, storing, distributing, operating, maintaining, modifying and disposing of a product."

Technical - Product definition information - information that defines the product's requirements, documents the product's attributes and is the authoritative source for configuration definition and control.

Technical - Product operational information - information used to operate, maintain and dispose the product.

Technical - Associated information - information generated as part of the product development and life-cycle management process, but isn't clearly definable as either of the other two categories.

The following sub paragraphs further delineate Technical-Product Data.

- **Technical Product - Definition Data**
  Examples of Technical-Product Definition Data include:

- **Design Information**
  Design Technical-product data Package (TDP) consisting of:
  - Drawings
  - 3-D CAD Drawings
  - Specifications
  - Lists
  - SW documentation
  - Interface Control Documents
  - Engineering Product Structure
- **Other Design Information**
  Other design information is related to the product and product decisions but not directly associated to the specification or design of the product. Examples consist of:
  - Trade Study Reports
  - Design Selection Worksheets
  - Engineering Analysis
  - Models and Test Cases
- **Requirements Information**
  Requirements information consists of originating requirements that the program uses as source documentation. The following are examples that a given program will need to maintain:
  - Requirements Document Information
  - Joint Capabilities Development System (JCIDS) Documents
  - Integrated Architecture Model Information and Views (AVs, OVs, SVs and TVs)
  - External Interface Control Documents
  - GFE/CFE Documentation
  - Other Requirements

    Other requirements are those requirements not specific to the product or implementation of the product. The following are examples:

    - Contract Statement of Work (SOW)
    - Process Standards (e.g. CMMi)

- **Technical-Product Operational Information**
  Technical-Product Operation Information is defined from the product definition information. Product operational information consists of procedures and technical information needed by operators and support personnel to operate, maintain and dispose of the product. Product operational information also includes field data that can be fed back into the product design improvement and the status accounting processes. Examples of Technical-Product Operational Information include:
  - **Logistics Management Information (LMI)**
    - Maintenance Planning Information
    - Technical Manuals

        - Interactive Electronic Manuals (IETMs)
        - Technical Publications
        - Support & Test Equipment Information
        - Supply Support Information
        - Manpower, Personnel & Training Information
        - Packaging, Handling, Storage & Transportation Information
        - Environment Safety & Occupational Health Information
        - Material IN-Service Information
        - Field Feedback Information
        - Demand Data from Field requisitions
        - Item Prognostics & Diagnostics Information
        - Field Quality Deficiency Reports
        - Product Unit Configuration Information
- **Technical-Product Associated Information**
  Technical-Product Associated Information is generated as part of product development and life-cycle management process, but isn't clearly definable as either product definition information or product operational information. This category of product data relates to the processes used in product definition, validation and operation, but doesn't necessarily directly describe the final product configuration.
  Examples of Technical-Product Associated Information are:
    - Test and Quality Assurance Information
    - Test Reports
    - System Evaluation Report
    - Configuration Control Information
    - Requirements for Changes
    - Requirements for Variance
    - CCB Decisions
    - Product Configuration Management Status
    - Other Associated Information
    - GIDEP Notices of Obsolete Parts
    - Supplier Notices of Obsolete Parts
    - Disposal Information
    - Related Contract ID Information

4.2.3.1.8. Interface Management

The interface management process ensures interface definition and compliance among the elements that compose the system, as well as with other systems with which the system or system elements will interoperate (i.e., system-of-systems (SoS)). Interface management control measures ensure that all internal and external interface requirement changes are properly documented in accordance with the configuration management plan and communicated to all affected configuration items.

Interface management deals with:

- Defining and establishing interface specifications,
- Assessing compliance of interfaces among configuration items comprising systems or system of systems,
- Monitoring the viability and integrity of interfaces within a system, and
- Establishing an interface management plan to assess existing and emerging interface standards and profiles, update interfaces, and abandon obsolete architectures.
- An interface management plan is a part of a configuration management plan that:
- Documents a system's internal and external interfaces and their requirement specifications,
- Identifies preferred and discretionary interface standards and their profiles,
- Provides justification for selection and procedure for upgrading interface standards, and
- Describes the certifications and tests applicable to each interface or standard.

The Interface Control Working Group (ICWG) is a specialized technical working group composed of appropriate technical representatives from the interfacing activities and other interested participating organizations. The ICWG serves as a forum to develop and provide interface requirements, as well as to focus on interface detail definition and timely resolution of issues The ICWG requires collaboration with external program offices and contractors in a system or system of systems environment.

Many of the external interfaces are identified through the Joint Capabilities Integration and Development System process and its accompanying documents and architectures. As system interface control requirements are developed, they are documented and made available to the appropriate stakeholders. Documented interface control requirements serve critical functions at all levels of the system. These interface control requirements are documented in an Interface Control Document and placed under configuration control. Some of these functions include:

- Facilitating competitive bids,
- Enabling integration of systems and sub-systems,
- Developing functional and physical architectures,
- Supporting system maintenance, future enhancement, and upgrades, and
- Providing input data for continuous risk management efforts.

Refinement of the interfaces is achieved through iteration. As more is learned about the system during the design phases, lower-level, verifiable requirements and interfaces are defined and refined. Impacts of the original defined capabilities and interfaces, performance parameter thresholds and objectives, and the system are evaluated when defining and modifying interfaces.

Interface management is a critical technical management process in a SoS. For individual systems, flexibility and stability of interfaces are mostly under individual program control. The dynamic nature and multi-constituent system construct of SoS makes successful interface management challenging and crucial. In a SoS, control of interface management will most likely be at the SoS level, while execution will likely be at the constituent system level.

4.2.3.2. Technical Processes

4.2.3.2. Technical Processes

The previous section on Technical Management Processes describes the eight technical management processes applied throughout the life cycle; this Section describes the eight technical processes. The program manager uses technical processes to design the system, subsystems, and components, including the supporting or enabling systems required to produce, support, operate, or dispose of a system. Section 4.5 discusses some key techniques and tools for conducting the analyses required in technical processes.

4.2.3.2.1. Stakeholder Requirements Definition Process

The Stakeholder Requirements Definition process elicits inputs from relevant stakeholders and translates the inputs into technical requirements. DoD systems engineers primarily respond to the Joint Capabilities Integration and Development System (JCIDS) documents that express the Concept of Operations (CONOPS) and identify capability gaps in need of a Materiel solution. The program manager and systems engineer will work with the user to establish and refine operational needs, attributes, performance parameters, and constraints that flow from JCIDS described capabilities, and then ensure that all relevant requirements and design considerations are addressed (see Figure 4.4.F1). The focus of this process should translate customer needs into the following program and system requirements:

- Performance parameter objectives and thresholds,
- Affordability constraints,
- Schedule constraints, and
- Technical constraints.

Once the program and system requirements are identified, documented, and coordinated with the stakeholders, the requirements need to be placed under change control so proposed changes can be carefully managed. Because the majority of the requirements will be defined through system decomposition at later stages of the program, iterative application of rigorous systems engineering is key. Stakeholder Requirements Definition complements the Requirements Analysis and Architectural Design technical processes. These three processes are recursively applied at each level of the system structure and then iteratively within each level throughout development. The objective is to help ensure that stakeholder requirements and capabilities are feasible and integrated as more information is learned about the requirements through analysis.

For a notional understanding of the emphasis of this process in relation to the acquisition phases, technical reviews, and baselines, refer to Section 4.2.4.1.

Role of DoDAF and Stakeholder Requirements Definition

The DoD Architecture Framework (DoDAF) defines a common approach for DoD architecture description development, presentation, and integration for both warfighting operations and business operations and processes. For Net Ready Key Performance Parameters, the Joint Capabilities Integration and Development System (JCIDS) and the DoDAF specify the required architecture products. The architecture products define the essential architecture views consisting of operational, system and technical views that express the net centric capabilities. The program manager and systems engineer need to work closely with the stakeholder to translate these architecture views into verifiable requirements.

4.2.3.2.2. Requirements Analysis Process

Requirements Analysis encompasses the definition and refinement of system, subsystem, and lower-level functional and performance requirements and interfaces to facilitate the Architecture Design process.

Requirements Analysis needs to provide measurable and verifiable requirements. Requirements should avoid specifying technological implementations. The requirements being developed by the materiel developer should balance requirements to include performance, functional and technical constraints, and both life-cycle costs and development cycle time.

The functional architecture is an essential aspect of the requirements analysis process. The nature of complex systems today requires a high degree of communication exchanges between distributed functions to achieve a given systems mission. This is extremely difficult to describe without the aid of a functional architecture that describes the organization of functions in the context of a desired operational mission or capability. A functional architecture expresses the detailed functional, interface, and temporal aspects of the system that are essential to gain sufficient insight and to communicate unambiguously the behavior of the system in its intended operational environment. The development of a functional architecture and definition of system functions should not be performed in isolation; it should be developed incrementally with

stakeholder requirements and the physical architecture to ensure that the appropriate functions and interfaces are identified. The application of rigorous functional analysis methods is essential in developing a good functional architecture. This analysis may utilize structured or object oriented methods, or a combination thereof, along with associated and proven notations such as Integration Definition for Function Modeling, Enhanced Functional Flow Block Diagram, and Systems Modeling Language.

The outcome of a functional architecture is the development of lower tier functional and performance requirements that need to be allocated to the system physical architecture. Requirements Analysis is a highly iterative process and tightly coupled to the Stakeholder Requirements Definition and Architectural Design processes. During this activity, missing, redundant or inconsistent requirements will most likely be discovered. In addition, the physical architecture may be affected based on a particular allocation approach which also requires resolution in parallel. This process is complete when the functional architecture is in balance with the stakeholder requirements.

The essential benefits of a functional architecture are that it provides for the following:

- A definition of the system functional baseline,
- A measure of the system's ability to fulfill its functional objectives as defined by the system functional requirements,
- A measure of the system's ability to fulfill its performance objectives as defined by the system performance requirements.
- The system's ability to operate within resource constraints,
- Costs, economic and otherwise, of implementing and operating the system over its entire life cycle, and
- Side effects, both positive and adverse, associated with architectural options

Definition of the functional architecture enables the following:

- Identifying functional interfaces and interactions between system elements (including human elements of the system) and with external and enabling systems,
- Defining the system integration strategy and plan (to include human system integration),
- Documenting and maintaining the functional architecture and relevant decisions made to reach agreement on the baseline functional design,
- Establishing and maintaining the traceability between requirements and system functions,
- Supporting the definition of verification and validation criteria for the system elements, and
- Performing what-if scenarios to explore stressing conditions to evaluate possible risks.

The objective of this process is to help ensure that the requirements derived from the customer-designated capabilities are analyzed, decomposed, functionally detailed across the entire system, feasible and effective.

For a notional understanding of the emphasis of this process in relation to the acquisition phases, technical reviews and baselines, refer to Section 4.2.4.1.

4.2.3.2.3. Architecture Design Process

The Architecture Design Process is a trade and synthesis process. It translates the outputs of the Stakeholder Requirements Definition and Requirements Analysis processes into alternative design solutions and selects a final design solution. The alternative design solutions include hardware, software, and human elements; their enabling processes; and related internal and external interfaces.

The development of the physical architecture consists of one or more logical models or views of the physical solution. The logical models or views may consist of conceptual design drawings, schematics, and block diagrams that define the systems form and the arrangement of the system components and associated interfaces. The development of a physical architecture is an iterative and recursive process and will evolve together with the requirements and functional architecture. Development of the physical architecture is complete when the system has been decomposed down to lowest system element or configuration item level, and it is critical that this process identify the design drivers as early as possible. Therefore, it is imperative that the driving requirements be identified and the combined processes—Stakeholder Requirements Definition, Requirements Analysis, and Architecture Design—will provide key insights to risk early in the development life cycle, allowing for mitigating strategies.

Key activities performed when developing a physical architecture and design include:

- Analysis and synthesis of the physical architecture and the appropriate allocation,
- Analysis of the constraint requirements,
- Identify and define physical interfaces and components, and
- Identify and define critical attributes of the physical components, including design budgets (e.g., weight, reliability) and open system principles.

In this process, derived requirements will come from design decisions. It is essential to identify derived requirements and ensure that they are traceable and part of the total requirements set. For each given alternative, the Decision Analysis process trades off the requirements and a given design alternative. For each alternative, based on programmatic decisions, certain requirements may be emphasized against the others. The essence of this activity is to achieve a balanced and feasible design within the program constraints. An integral part of defining and refining the functional architecture, physical architecture design is to provide technical support to the market research required early in the program life cycle. Systems engineers within DoD conduct architecture design tasks similar to what their commercial counterparts encounter in addressing market research and customer needs. These tasks involve analyzing if and how an existing product (commercial or non-developmental item) can meet user requirements. Systems engineers need to consider mature technologies to meet user requirements.

The development of the system architecture should adhere to sound systems engineering. At a minimum, a system architecture contains the definition of the system requirements, functional and physical architectures that define the functional, allocated, and product baselines. The functional architecture should be part of the functional baseline, and the physical architecture should be part of the allocated and product baselines. The system architecture is maintained in a robust repository that maintains the architecture descriptions, its relationships to the technical baselines, and ensures consistency of the system's architecture definition over its life cycle.

If the process finds that specified objectives and thresholds are ineffective or unsuitable, it may then be necessary to reevaluate the defined performance parameters.

The output of this process is the physical design that results in design definition documentation such as specifications, allocated and product baselines, and Work Breakdown Structures. Physical architectures and the resulting design should be sufficiently detailed to allow the following:

- Confirmation of upward and downward traceability of requirements, across the functional, allocated, and product baselines
- Confirmation of interoperability and open system performance requirements, and
- Sufficient product and process definition to support implementation, verification, and validation of the design.

Confirmation of requirements traceability and the soundness of the selected physical design can be accomplished using a cost effective combination of design analysis, design modeling, and simulation, as applicable.

For a notional understanding of the emphasis of this process in relation to the acquisition phases, technical reviews, and baselines, refer to Section 4.2.4.1.

4.2.3.2.4. Implementation Process

Implementation is the process that actually yields the lowest level system elements in the system hierarchy. The system element is made, bought, or reused. Making it involves the hardware fabrication processes of forming, removing, joining, and finishing; or the software processes of coding, etc. If implementation involves a production process, a manufacturing system needs to be developed using the established technical and technical management processes.

Depending on the technologies and systems chosen when a decision is made to produce a system element, the implementation process imposes constraints on the Architecture Design process. If the decision is made to purchase or reuse an existing system element, the implementation process may involve some adaptation or adjustments to the system element. The Implementation process gets the system element ready for the processes of integration, verification, and validation. The implementation process should include some testing of the implemented system element before the element passes to the integration process. Implementation may also involve packaging,

handling, and storage, depending on where or when the system element needs to be integrated into a higher-level assembly. Developing the supporting documentation for the system element, such as the manuals for operation, maintenance, and/or installation, is also a part of the implementation process.

For a notional understanding of the emphasis of this process in relation to the acquisition phases, technical reviews and baselines, refer to Section 4.2.4.1.

4.2.3.2.5. Integration Process

Integration is the process of incorporating the lower level system elements into a higher-level system element in the physical architecture. The plan or strategy for the integration process, including the assembly sequence and the human interface during operational use, may impose constraints on the physical architecture and the design. An assembled system element may include fixtures for hardware or compilers for software, also developed with the technical and technical management processes.

The integration process will be used with the transition process for the incorporation of the final system into its operational environment to ensure that the system is integrated properly into all defined external interfaces, including human, hardware, and software.

The interface management process is particularly important for the success of the integration process, and iteration between the two processes will occur.

For a notional understanding of the emphasis of this process in relation to the acquisition phases, technical reviews and baselines, refer to Section 4.2.4.1.

4.2.3.2.6. Verification Process

The Verification Process confirms that the system element meets the design to or build-to specifications as defined in the functional, allocated, and product baselines. System element also includes tools and support items used in development and test such as simulation models and system development/integration laboratories. It answers the question "Did you build it right?" As such, it verifies the system elements against their defined requirements (build-to specifications). Activities performed in the verification process include:

- **Verification Planning:** Verification planning is performed at each level of the system under development. For example, a typical level to a given system will consist of system, segment, subsystem and component levels. For each level of the system under development, a separate verification plan is created. The following activities describe the developing a verification plan:
    - **Verification Method and Level Assignments:** Defines the relationships between the specified requirements consisting of functional, performance, constraints, and

the associated method and level of verification. This activity typically yields a Verification Cross Reference Matrix for each level of the architecture and serves as the basis for definition of the verification tasks. The level of verification is assigned consistent with the level of requirement (e.g., system level, subsystem level etc.). The typical methods of verification are demonstration, inspection, analysis, and test.

- Demonstration. Demonstration is the performance of operations at the system/sub-system level where visual observations are the primary means of verification. Demonstration is used when quantitative assurance is not required for verification of the requirements.
- Inspection. Visual inspection of equipment and evaluation of drawings and other pertinent design data and processes will be used to verify conformance with characteristics such as physical, material, part and product marking and workmanship.
- Analysis. Analysis is the use of recognized analytical techniques (including computer models) to interpret or explain the behavior/performance of the system element. Analysis of test data or review and analysis of design data will be used as appropriate to verify requirements.
- Test. Test is an activity designed to provide data on functional features and equipment operation in an operational environment under fully controlled and traceable conditions. The data is subsequently used to evaluate quantitative characteristics. Evaluation includes comparison of the demonstrated characteristics with requirements. Tests are conducted when an acceptable level of confidence cannot be established by other methods, or if testing can be shown to be the most cost effective method.

  - **Verification Task Definition:** Defines all verification tasks with each task addressing one or more requirements. The ability of defining good verification tasks requires the test engineer to have a sound understanding of how the system is expected to be used and its associated environments. An essential tool for the test engineer is to utilize the integrated architecture that consists of the requirements, functional and physical architectures. The functional architecture is used to support functional and performance test development and in combination with the physical architecture, a family of verification tasks are defined that that will verify the functional, performance and constraint requirements.
  - **Verification Configuration Definition:** Defines the technical configuration, resources, including people, and environments needed to support a given verification task. This may also include hardware or software to simulate the external interfaces to the system to support a given test.
  - **Verification Scheduling**: Defines the schedule for the performance of the verification tasks and determines which verification tasks are in sequence or in parallel and the enabling resources required for execution of the verification tasks.

- **Verification Execution:** The performance of a given verification task with supporting resources. The verification task results, whether from a test, analysis, inspection or

simulation, are documented for compliance or non-compliance with data supporting the conclusion.

- **Verification Reporting:** Reports the compiled results of the executed verification plan and verifies the materials employed in system solutions can be used in a safe and environmentally compliant manner.

The nature of verification activities changes as designs progress from concept, through detailed designs, to physical products. Throughout the system's life cycle, however, design solutions at all levels of the physical architecture are verified through a cost-effective combination of analysis, examination, demonstration, testing and evaluation, all of which can be aided by modeling and simulation.

For a notional understanding of the emphasis of this process in relation to the acquisition phases, technical reviews and baselines, refer to section 4.2.4.1.

4.2.3.2.7. Validation Process

The Validation Process answers the question of "Is it the right solution to the problem?" As such, this process works in conjunction with the Stakeholder Requirements, Requirements Analysis and Architecture and Design processes. It evaluates the requirements, functional and physical architectures and ultimately evaluates the implementation. In the early stages of the system development life cycle, validation may involve independent evaluation of the system requirements, development of prototypes and simulations all with the purpose of validating the system concept.

For a notional understanding of the emphasis of this process in relation to the acquisition phases, technical reviews and baselines, refer to Section 4.2.4.1.

4.2.3.2.8. Transition Process

Transition is the process applied to move any system element to the next level in the physical architecture. For the end-item system, it is the process to install and field the system to the user in the operational environment. The end-item system may need to be integrated with other systems in the operational environment honoring the defined external interfaces. In this case, the transition process will need be performed in conjunction with the integration process and interface management process for a smooth transition.

For a notional understanding of the emphasis of this process in relation to the acquisition phases, technical reviews and baselines, refer to Section 4.2.4.1.

4.2.4. Application of Systems Engineering Processes

4.2.4. Application of Systems Engineering Processes

Overall, the flow of the systems engineering processes is iterative within any one phase of the acquisition process and is recursive at lower and lower levels of the system structure. Systems engineering processes are applied to allow an orderly progression from one level of development to the next more detailed level through the use of functional, allocated, and product baselines under proper configuration management. These processes are used for the development of system, subsystems, and system components as well as for the supporting or enabling systems used for the testing, production, operation, training, support, and disposal of that system. If during the course of technical management processes and activities, such as trade studies or risk management activities, specific requirements, interfaces, or design solutions may be identified as non-optimal and subsequently changed to increase system-wide performance, achieve cost savings, or meet scheduling deadlines. These processes not only transition requirements from design to system, but also serve as an integrated framework within which the universe of requirements is, as a collective whole, defined, analyzed, decomposed, traded, managed, allocated, designed, integrated, tested, fielded, and sustained.

4.2.4.1. Systems Engineering Technical Processes, Technical Reviews and Baselines

While the systems engineering technical processes are life-cycle processes, the processes are concurrent and the emphasis of the respective processes depends on the phase and maturity of the design. Figure 4.2.4.1.F1 demonstrates (going from left to right) a notional emphasis of the respective processes throughout the acquisition life cycle.

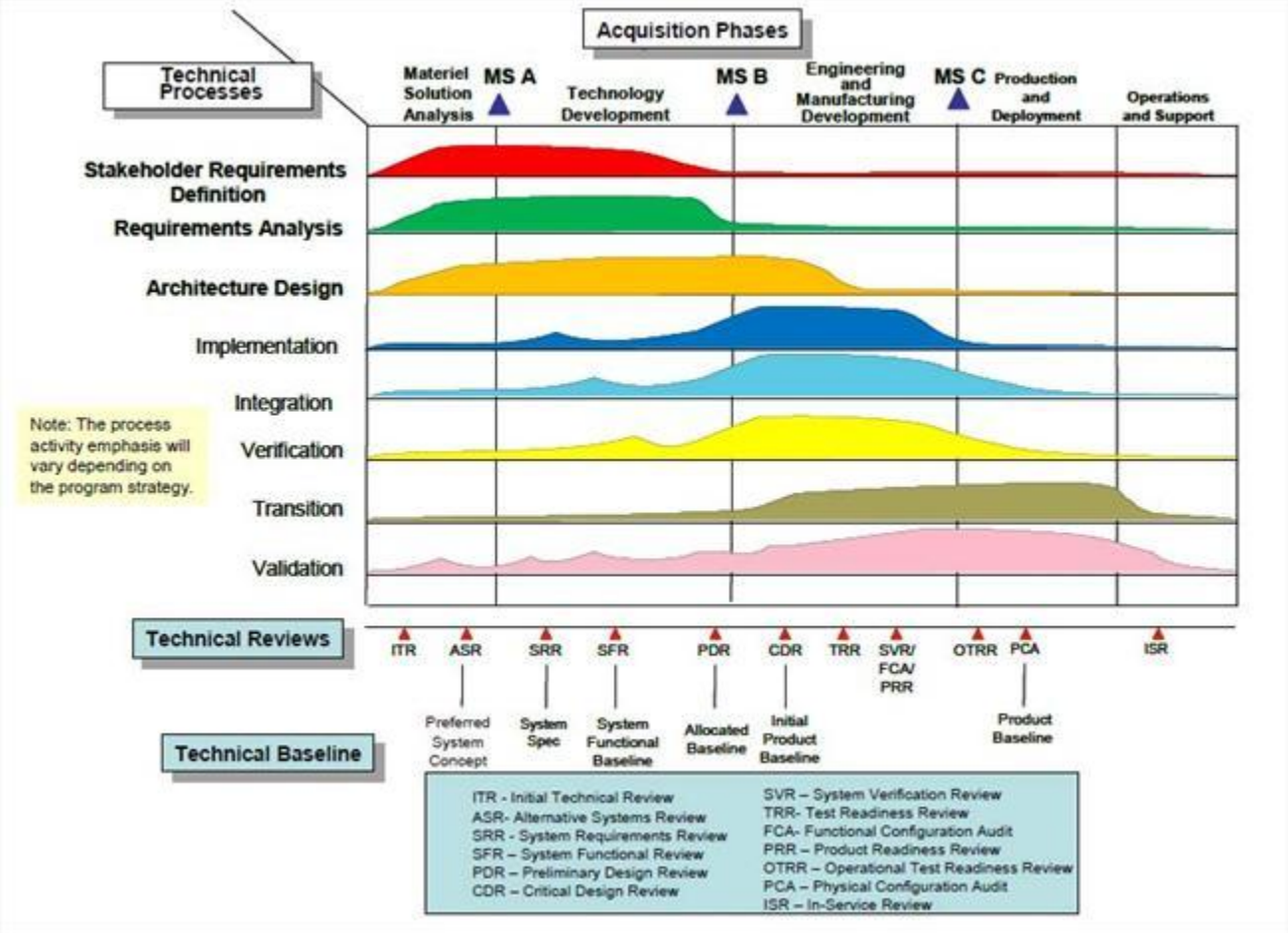


Figure 4.2.4.1.F1. Notional Emphasis of Systems Engineering Technical Processes and the Acquisition Life Cycle

4.3. Systems Engineering Activities in the System Life Cycle

The DoD Instruction 5000.02 establishes the framework for acquisition programs. These programs are structured in phases, each separated by milestone decisions. In each phase of a system's life cycle, from concept to disposal, there are important systems engineering actions that, if properly performed, will assist the program manager in managing the program. The quality of products is determined by the extent they meet (or exceed) requirements and satisfy the customer(s), at an affordable cost. A key to program success is to incorporate systems engineering design quality into the product by defining the product requirements as early as possible.

This section acquaints program managers with the variety of acquisition documents that have systems engineering implications, either as sources of system parameters (e.g., the Initial

Capabilities Document and Capabilities Development Document) or as the recipients of systems engineering analyses outputs (e.g., acquisition strategy, analysis of alternatives, etc.). This section illustrates how the systems engineering processes of Section 4.2 can be applied and tailored to each acquisition phase:

- Each phase builds upon the previous phase to further define the system technical solution,
- Systems engineering processes are iterated at each system element level, and
- Technical reviews serve to confirm major technical efforts within the acquisition phases, affirm outputs of the acquisition phases, and progress toward the next acquisition phase. Failure to complete a technical review does not preclude the initiation of follow-on activity, but does preclude the commitment to a baseline (e.g., initial fabrication may begin before establishment of the product baseline at Critical Design Review, but all should recognize that the review may approve a different baseline).

As the by-phase discussions illustrate, there are a number of technical reviews appropriate to each acquisition phase that are conducted at all appropriate levels within a program.

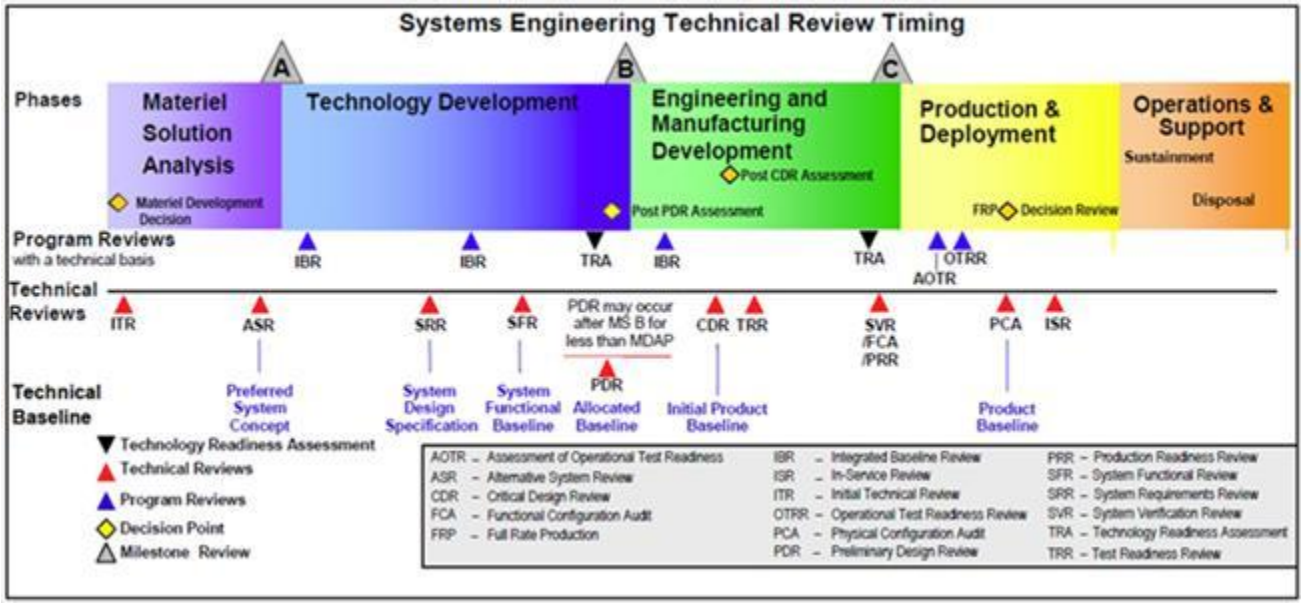
DoD Instruction 5000.02, Enclosure 12, paragraph 4, directs that:

Technical reviews of program progress shall be event driven and conducted when the system under development meets the review entrance criteria as documented in the SEP. They shall include participation by subject matter experts who are independent of the program (i.e., peer review), unless specifically waived by the SEP approval authority as documented in the SEP.

Technical reviews should be:

- Event-driven vice schedule-driven,
- Conducted when the system under development satisfies review entry criteria as documented in the Systems Engineering Plan ,
- Conducted, at a minimum, at the transition from one acquisition phase to the next and at major transition points of the technical effort (e.g., from preliminary to detailed design at Preliminary Design Review), and
- Required by contractual documents and have technical review processes and requirements included.

Figure 4.3.F1 shows the relative timing of each of the technical reviews, technically oriented program reviews, and technology readiness assessments.



To assist in the preparation for and conduct of technical reviews technical review risk assessment checklists are available for each of the reviews. These checklists are designed as a technical review preparation tool, and should be used as the primary guide for the risk assessment during the review. The checklist itself can be both an input to, and an output of, the review. The Integrated Product Team can do a self-assessment as input, but the review participants should take ownership of the assessed risk as an output of the review. These checklists are available on the Systems Engineering Community of Practice and are accessible in the DAU Technical Reviews Continuous Learning Module, CLE-003.

DoD Instruction 5000.02, Enclosure 4, presents the statutory, regulatory, and contract reporting information and milestone requirements for acquisition programs. These requirements are significant, and, in some cases, the lead-time for preparation may exceed one year. The information and/or decisions that a program office reports in these documents often rely on analyses begun in pre-acquisition. During pre-acquisition, systems engineering processes translate user-defined capabilities into system specifications. As explained earlier, the systems engineering process is conducted through both iterative and recursive activities. Likewise, some of the information requirements are iterative by milestone. Throughout this section, the terminology used to indicate a subsystem is a system element, component, or configuration item, depending on the systems engineering context and phase of acquisition under discussion. Throughout this document, the term configuration item generally refers to both software and hardware items.

4.3.2. Technology Development Phase

A successful Milestone A decision initiates the Technology Development phase. Per DoD Instruction 5000.02, this phase matures technologies, determines the appropriate set of technologies to be integrated into a full system, conducts competitive prototyping of system elements, refines requirements, and develops the functional and allocated baselines of the end-item system configuration. If a platform or system depends on specific technologies to meet system operational threshold requirements in development, production, operation, and sustainment, and if the technology or its application is either new or novel, then that technology is considered a critical or enabling technology. If there are any critical technology elements, they are to be evaluated during the Technology Development phase to assess technology maturity. Technology Development is a focused effort to mature, prototype, and demonstrate technologies in a relevant environment. This results in a preferred system concept that achieves a level suitable for low risk entry into Engineering and Manufacturing Development. This can best result from a close collaboration between the science and technology community, the user, and the engineering community.

This phase develops and demonstrates prototype designs to reduce technical risk, validate designs, validate cost estimates, evaluate manufacturing processes, and refine requirements. Based on refined requirements and demonstrated prototype designs, Integrated Systems Design of the end-item system can be initiated. When approved in the Technology Development Strategy, the Integrated Systems Design may be conducted prior to Milestone B, to include full functional analysis of the end-item system, definition of the functional baseline, following the System Functional Review; functional allocation to system configuration items; and establishment of the system allocated baseline following the Preliminary Design Review. Additionally, the Technology Development Phase efforts ensure the level of expertise required to operate and maintain the product is consistent with the force structure. Technology development is an iterative process of maturing technologies and refining user performance parameters to accommodate those technologies that do not sufficiently mature (requirements trades). The Initial Capabilities Document, the Technology Development Strategy, and the maturing draft Capability Development Document (CDD) guide the efforts of this phase, leading to the approved CDD.

Competitive prototyping and effective employment of systems engineering, applied in accordance with a well-structured Systems Engineering Plan, and monitored with meaningful technical reviews, will reduce program risk, identify potential management issues in a timely manner and support key program decisions.

4.3.2.1. Purpose of Systems Engineering in Technology Development

During the Technology Development phase, systems engineering provides comprehensive, iterative processes to accomplish the following activities:

- Convert each required capability into a system performance requirement,
- Align user-defined performance parameters against enabling/critical technology solutions,

- Integrate evolving and mature technologies into competitive, technically mature prototyping of key system elements,
- Evaluate prototyped solutions against performance, cost, and schedule constraints to balance the total system solution space,
- Develop a system performance specification that balances achievable performance with cost, schedule, and other constraints
- Characterize and manage technical risk including producibility risk,
- Characterize and assess ESOH risks for both evolving and mature technology solutions
- Transition mature technology from the technology base into program specific efforts,
- When approved in the Technology Development Strategy, conduct Integrated System Design of the system to include functional analysis, definition of the functional baseline, and preliminary design,
- Verify that the system preliminary design and allocated baseline are sufficiently mature to enter into Engineering and Manufacturing Development, and
- Assess the industrial base to identify potential manufacturing sources.

Systems engineering processes mature, prototype, and demonstrate the suite of selected system elements and complete the preliminary design of the full system for low-risk entry to Engineering and Manufacturing Development. Competitive Prototyping considerations are critical to program risk reduction and require thorough Technical Planning and detailed implementation in the Technology Development Phase.

Competitive Prototyping considerations include the following:

- Decide what should be prototyped: program issues should drive the prototyping scope,
- Encourage alternate choices on solutions to achieving capability,
- Know the purpose for prototyping (is it risk reduction, i.e., cost, size, technology maturation, assess design viability, schedule, manufacturability, demonstrate integration, etc…),
- Prototype the items that are unique to the program or project,
- Address Technology Readiness Level (TRL) maturity concerns,
- Ensure competition and use prototyping as part of the overall program risk management,
- Use competitive prototyping to create increased corporate interest,
- Do proof of concept but also address the other critical risks,
- Shape prototyping strategy at pre-milestone "0" by identifying the key things that must be solved. Build prototypes and find the problems early,
- Doing the "right" prototyping is key. Prototype when you cannot model. Determine the right time for prototyping, and
- Know your prototyping purpose. Decompose the requirements. Prototype to create and sell the product.

4.3.2.2. Inputs to the Systems Engineering Processes in Technology Development

The following information sources provide important inputs to the systems engineering processes supporting Technology Development:

- Initial Capabilities Document and draft Capability Development Document,
- Approved Materiel Solution,
- Exit Criteria,
- Test and Evaluation Strategy,
- System Safety Analyses to include initiation of Safety Requirements/Criteria Analysis and update the Preliminary Hazard List for the preferred concept,
- Support and Maintenance Concepts and Technologies,
- Analysis of Alternatives (AoA),
- Systems Engineering Plan, and
- Technology Development Strategy.

4.3.2.3. Key Systems Engineering Activities During Technology Development

4.3.2.3.1. Interpret User Needs; Analyze Operational Capability and Environmental Constraints

4.3.2.3.2. Develop System Performance (and Constraints) Specifications and Enabling/Critical Technologies and Prototypes Verification Plan

4.3.2.3.3. Develop Functional Definitions for Enabling/Critical Technologies/Prototypes and Associated Verification Plan

4.3.2.3.4. Decompose Functional Definitions into Critical Component Definition and Technology Verification Plan

4.3.2.3.5. Design/Develop System Concepts, i.e., Enabling/Critical Technologies; Update Constraints and Cost/Risk Drivers

4.3.2.3.6. Demonstrate Enabling/Critical Technology Components Versus Plan

4.3.2.3.7. Demonstrate System and Prototype Functionality Versus Plan

4.3.2.3.8. Demonstrate/Model the Integrated System Versus the Performance Specification

4.3.2.3.9. Demonstrate and Validate the System Concepts and Technology Maturity Versus Defined User Needs

4.3.2.3.10. Transition to Integrated System Design

4.3.2.3.11. Interpret User Needs, Refine System Performance Specifications and Environmental Constraints

4.3.2.3.12. Develop System Functional Specifications and Verification Plan to Evolve System Functional Baseline

4.3.2.3.13. Evolve Functional Performance Specifications into System Allocated Baseline

4.3.2.3. Key Systems Engineering Activities During Technology Development

The systems engineering-related steps during the Technology Development phase are identified in Figure 4.3.2.3.F1. Note: Given the iterative and recursive nature of systems engineering, the sequence of activities (displayed in the highlighted rectangles) is in their order of completion, vice the order of commencement. The activities can be started in any order and often run in parallel, but should be completed in the order shown. Paragraphs below contain additional detail on each step.

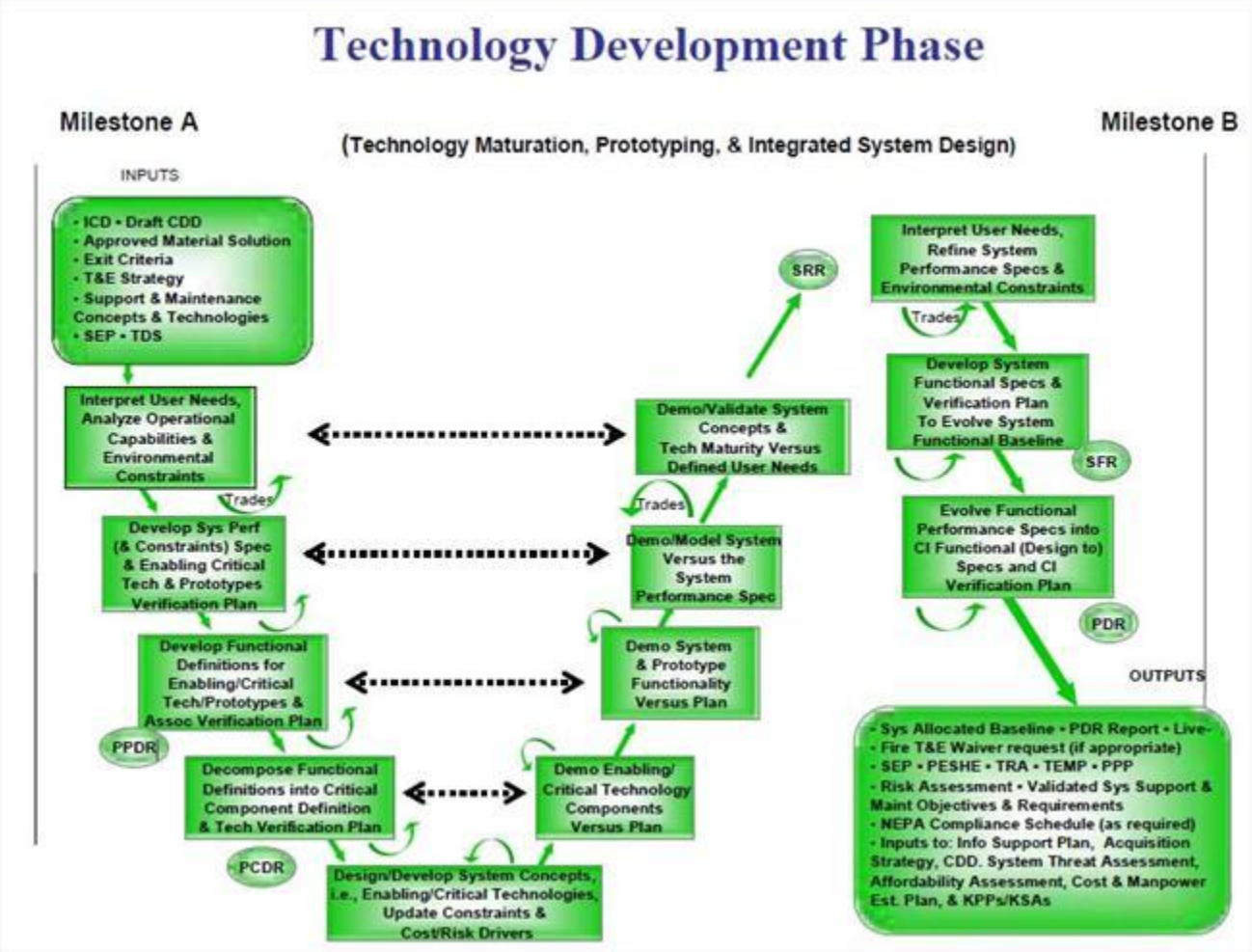


Figure 4.3.2.3.F1. Systems engineering-related steps during Technology Development

4.3.2.3.1. Interpret User Needs; Analyze Operational Capability and Environmental Constraints

This step includes the aggregation of all inputs available at this stage of the program (Initial Capabilities Document, draft Capability Development Document, results of the Analysis of Alternatives (AoA) and identification of the approved materiel solution, exit criteria for the phase, Systems Engineering Plan including competitive prototyping planning, Technology Development Strategy, Test and Evaluation Strategy, as well as associated support and maintenance concepts and technologies, training system, and interoperable systems). Additional analysis and definition may be required to ascertain all of the related constraints to be applied to the effort:

- Environmental-systems threats, usage environment, support environment, doctrine, operational concepts (including installation/range Environmental, Safety and Occupational Health asset requirements), etc.,
- Resource-industrial base, notional available development, operation, and support budgets, anticipated manning, and the required date for system fielding (e.g., Initial Operational Capability or Full Operational Capability),
- Technology-applicable technology base to be used for technology development and prototyping, and
- Statutory and regulatory: applicable titles of the United States Code (USC) and public laws, the Federal Acquisition Regulation (FAR), the DoD 5000-series, etc.

Key to this technology development effort is ensuring that all aspects of the required technologies are adequately matured, prototyped where appropriate, and managed as an integrated whole, and can support the user needs via the approved materiel solution (both the weapon system and its support concept). During this phase, this is accomplished through competitive prototyping and demonstrating the maturity of critical enabling technologies. This not only ensures that overall expectations are explicitly defined but also that trade space and risk in each of the areas above are defined. This will enable comprehensive analysis of technology availability and rational formulation of a system performance specification that strikes the best balance in meeting all of the needed capabilities with achievable performance, and within the many constraints on the program.

4.3.2.3.2. Develop System Performance (and Constraints) Specifications and Enabling/Critical Technologies and Prototypes Verification Plan

This step includes the further analysis and decomposition (from capability level to system level) of system performance and system design constraints, traceable back to those capabilities and constraints defined above. All capabilities and environmental constraints should be decomposed to the system performance level. They should be re-analyzed to determine the extent to which available technologies can meet the full spectrum of needs and constraints (as needs and

constraints become better understood as a result of decomposition). The trade space and risk should be analyzed and assessed against available technologies. The enabling and/or critical technologies should be identified. Each technology performance capability should be explicitly defined and related to the capability needs. To the extent performance can only be met through trade-offs of certain aspects (because of incompatibility of capabilities/constraints), changes may be required to the capability or constraints previously defined.

Verification planning should define test and evaluation requirements to demonstrate the ability of enabling and/or critical technologies to meet system requirements.

4.3.2.3.3. Develop Functional Definitions for Enabling/Critical Technologies/Prototypes and Associated Verification Plan

This step requires the further decomposition of system performance to the functional level. The functional requirements should be evaluated against available technologies, such that enabling and/or critical technologies can be defined. Consideration should be given to inclusion of functionality and functional flow definition across the full system (e.g., tactical system, support system, training system, etc.) and how this functionality relates to other interoperable systems (functional interfaces). Critical to this analysis is an understanding of the level of functionality achievable within the program constraints and program risk. Trade space (i.e., available designs that meet full set of threshold requirements) and risk should be analyzed and assessed against desired functional performance. Trade-offs (i.e., more conservative adjustments to some requirements thresholds) may be required to stay within program constraints and may require changes to higher-level system definitions.

A System Functional Review of a defined functional baseline may be conducted to support the development of the prototype system, subsystem(s), assemblies, or component(s). System functional verification planning should develop test and evaluation requirements to demonstrate system functionality and the maturity of the enabling/critical technologies.

4.3.2.3.4. Decompose Functional Definitions into Critical Component Definition and Technology Verification Plan

This step includes the allocation of system functions into critical components of the system that will provide the required functionality. Key to this analysis is an understanding of what functional performance is enabled by multiple sub-systems, or system components, operating as a functional entity. Hardware elements, software elements, physical interfaces, functional interfaces, standards, and existing and to-be-developed technology elements should all be considered and defined in the system specification. As in previous steps, this level of decomposition and allocation may induce requirements trades to stay within program constraints. These trades should be reflected in higher-level functional, system, capability definitions, and system specifications (i.e., these engineering entities should be updated accordingly).

A Preliminary Design Review of a defined allocated baseline may be conducted to support the development of the prototype system, subsystems, assemblies, or components.

System component verification planning should enable test and evaluation to validate critical system components and prototype demonstrations.

4.3.2.3.5. Design/Develop System Concepts, i.e., Enabling/Critical Technologies; Update Constraints and Cost/Risk Drivers

At this point, all of the basic system design requirements should have been analyzed, defined, and reconciled with constraints. The system components are synthesized and substantiated (e.g., through analyses, modeling and simulation, prototyping, demonstrations, etc.) to allow verification of the components against requirements, and integration of the components into an overall system for further validation.

A Critical Design Review of a defined initial product baseline may be conducted to support development of the prototype system, subsystems, assemblies, or components. Key to this step is the development of system concepts and prototypes that will demonstrate the viability of the overall system, indicate where enabling and/or critical technology maturation should occur, and validation that acceptable trade requirements space (i.e., sufficiently conservative requirements) to support low-risk entry to Engineering and Manufacturing Development.

4.3.2.3.6. Demonstrate Enabling/Critical Technology Components Versus Plan

Using the system component verification planning developed as part of the prototype allocated baseline, the system elements enabling/critical technology components should be evaluated. Evaluation results should be assessed against system component requirements, and the impact on the overall system capabilities and constraints determined. Critical to this step is the understanding of test and evaluation results and how well the system component functionality demonstrates desired capabilities, as well as what enabling and/or critical component technologies are required and the level of achievable performance. Trade-offs to system capability or additional system component development may be required, including adjustments to program and system constraints.

4.3.2.3.7. Demonstrate System and Prototype Functionality Versus Plan

Using the system functional verification plans developed as part of the functional baseline, the overall prototype functionality should be tested and evaluated, including prototype demonstration and assessment. System components are integrated and assessed from a functional standpoint relative to desired capabilities. Critical to this step is the understanding of how the

enabling components work together as an integrated whole to enable functionality at the prototype system, subsystem, assembly or component level, and how the achieved functionality relates to the overall desired system capability. Also important is an understanding of the enabling and/or critical technology maturity required to achieve critical functions. Trade-offs of desired capability, or further refinement of functionality, may be required, including adjustments to program and system constraints.

4.3.2.3.8. Demonstrate/Model the Integrated System Versus the Performance Specification

Using Engineering Development Models (EDMs) and prototypes, modeling and simulation, and the verification objectives previously defined, the overall integrated system should be evaluated against system performance objectives and constraints. System components are integrated from both physical and functional perspectives across the full system domain (tactical, support, training, etc.). Critical to this step is an understanding of the capability of the overall system versus need, the level of achievable performance within the complete set of constraints, and the enabling/critical technologies requiring further development. Trades at this level will include decisions as to acceptable technology risk versus desired system performance. If any technology is not mature enough to be included in the current increment system, an off-ramp technology to mitigate risk should be identified. Immature technology should be deferred to later increments of the system.

4.3.2.3.9. Demonstrate and Validate the System Concepts and Technology Maturity Versus Defined User Needs

Based upon the results of the verification of components, functionality, and system performance, a System Performance Specification should be created. Trade-offs of achievable performance should be complete and captured in the Systems Specification. Critical and/or enabling technologies should have demonstrated adequate maturity to achieve low-risk entry into the following phases of acquisition, described below.

4.3.2.3.10. Transition to Integrated System Design

Based upon the results of the competitive prototyping efforts and the success/failure of those prototypes to meet requirements, trades are made in the technical approach and cost and schedule constraints relative to full system development. This may involve adjustments to top-level requirements, revised cost and schedule estimates, and other constraints based on prototype results. Achieved technical and management performance should be reflected in the plan forward to a low-risk initial full system development (full system functional analysis, system-level functional baseline definition, full system functional allocation, and definition of the system-level allocated baseline). The System Performance Specification serves as the guiding technical requirement for the start of the Integrated System Design effort, leading up to an including the Preliminary Design Review.

4.3.2.3.11. Interpret User Needs, Refine System Performance Specifications and Environmental Constraints

This step includes understanding all of the inputs available at this stage of the program, including the Initial Capabilities Document, a draft Capability Development Document, Acquisition Program Baseline, Systems Engineering Plan (SEP), Test and Evaluation Master Plan, as well as validated system support and maintenance concepts and technologies. The users and the requirements authority have already approved a minimum set of Key Performance Parameters that are included in the draft Capability Development Document that guide the efforts of this phase. As the design matures, the program manager may conduct trade studies on the threshold and objective levels, and refine the key performance parameters thresholds and objectives with the approval of the requirements authority.

Throughout these activities, the program manager should maintain a thorough understanding of the key performance parameters, certification requirements, other specified performance parameters, and the suite of matured technologies resulting from the Technology Development phase. The program manager should ensure that all aspects of the specified system are adequately matured and managed as an integrated whole. The refined system specifications should consider all life-cycle processes and constraints, such as system availability, supportability, logistics footprint, training, and other logistics requirements, developmental and operational test environments and scenarios, and disposal.

For example, the program manager should plan the Programmatic Environmental, Safety and Occupational Health Evaluation. The program manager should develop and manage the system requirements stemming from the life-cycle considerations, and use prototypes to ensure user and other stakeholder buy-in as the design matures. The program manager should continually update cost and schedule estimates synchronized with SEP and other program plans. The program manager should continually address and characterize technical risk, and prepare for an additional System Requirements Review (SRR), if required. The purpose of an SRR at the early stages of Engineering and Manufacturing Development (EMD) is to set the detailed system requirements at a time when the supplier team for EMD is in place, and to ensure that the top level requirements are consistent with and in alignment with the contract requirements.

4.3.2.3.12. Develop System Functional Specifications and Verification Plan to Evolve System Functional Baseline

This step decomposes the required system requirements based on the draft Capability Development Document performance parameters and all other requirements and constraints, and derives detailed functional requirements for the system. This functional analysis and decomposition establishes the system functional baseline for the System Functional Review (SFR) that follows this step. The program manager should ensure that the program team continually monitors system cost, schedule, and risk against the evolving functional baseline to ensure that the decomposed functionality is consistent with program constraints. The program

manager should factor appropriate requirements considerations into trade studies, and incorporate them into the functional baseline.

The program manager should develop plans for system verification, and include these plans as part of the approved functional baseline, following the SFR. The verification planning should consider all interface functional and performance specifications.

4.3.2.3.13. Evolve Functional Performance Specifications into System Allocated Baseline

This step involves allocating functional performance specifications into system functional and performance requirements allocated across the system down to a configuration item level. Functions are allocated to each configuration item yielding "design to" preliminary design specifications and verification plans at the configuration item level. Mature technologies, the envisioned operational environment(s), design considerations and the other logistics and product support elements should be part of satisfying performance and supportability needs. The program manager should plan to test and evaluate to verify the configuration items (hardware and software) for functionality and performance. The program manager should ensure the program team monitors cost, schedule, and performance against the allocated baseline. Additional sustainment related analyses conducted at this step include a Failure Mode Effects and Criticality Analysis, a Fault Tree Analysis, and a Reliability-Centered Maintenance Analysis.

A system level Preliminary Design Review shall be conducted to approve and establish the allocated baseline for the overall system. This review culminates the individual PDR for each configuration item of the overall system level. The allocated baseline includes all functional and interface characteristics from the system, interface requirements with other configuration items, and design constraints, captured in preliminary design specifications. The allocated baseline should also describe the verification required to demonstrate the achievement of specified functional and interface characteristics.

4.3.2.4. Technical Reviews During Technology Development

4.3.2.4. Technical Reviews During Technology Development

The technical reviews during the Technology Demonstration phase will provide for the definition, development, and demonstration of prototypes of system, subsystem, assembly, and/or component. The scope of all Technology Demonstration phase technical reviews will be consistent with the Technology Development Strategy, Test and Evaluation Strategy, and Systems Engineering Plan. As such, the program may start or complete the initial system design effort up to and including the System Prototype Design Review.

4.3.2.4.1. Technical Reviews to Support Prototyping

The definition, development, and demonstration of prototypes of system, subsystem, assembly, and component may require the application of systems engineering technical management processes and technical processes and appropriate prototype technical reviews. Technical reviews in support of competitive prototyping and systems engineering technical reviews such as Prototype Functional Review, Prototype Preliminary Design Review or Prototype Critical Design Review, can be beneficial to support the technical approach and program plans. Application of these reviews are at the discretion of the program office and prototype developer and should follow the guidance herein as presented for these reviews, which are discussed only in the context of full system development.

4.3.2.4.2. Technical Reviews to Start Integrated System Design

4.3.2.4.2.1. System Requirements Review (SRR)

The SRR is a multi-disciplined technical review to ensure that the system under review can proceed into initial systems development, and that all system requirements and performance requirements derived from the Initial Capabilities Document or draft Capability Development Document are defined and testable, and are consistent with cost, schedule, risk, technology readiness, and other system constraints. Generally this review assesses the system requirements as captured in the system specification, and ensures that the system requirements are consistent with the approved materiel solution (including its support concept) as well as available technologies resulting from the prototyping effort.

Of critical importance to this review is an understanding of the program technical risk inherent in the system specification and in the Engineering and Manufacturing Development (EMD) phase Systems Engineering Plan (SEP). Determining an acceptable level of risk is essential to a successful review.

Completion of the SRR should provide the following:

1. An approved system performance specification with sufficiently conservative requirements to provide for design trade space for the EMD phase,
2. A preliminary allocation of system requirements to hardware, human, and software subsystems,
3. A preliminary Identification of all software components (tactical, support, deliverable, non-deliverable, etc.),
4. A comprehensive risk assessment for EMD,
5. An approved EMD phase SEP that addresses cost and critical path drivers, and
6. An approved Life-cycle Sustainment Plan defining the product support plan and sustainment concepts with the corresponding metrics.

The SRR is conducted to ascertain progress in defining system technical requirements. The SRR is intended to confirm that the user's operational requirements are sufficiently well understood and have been translated into system specific technical requirements to permit the developer (contractor) to establish an initial system level requirements baseline. It determines the direction and progress of the systems engineering effort and the degree of convergence upon a balanced and complete configuration baseline. It is normally held during the Technology Development phase, but it may be repeated after the start of EMD to clarify the contractor's understanding of redefined or new user requirements.

During the SRR, the systems requirements are evaluated to determine whether they are fully defined and consistent with the mature technology solution, and whether traceability of systems requirements to the Initial Capabilities Document or draft Capability Development Document is maintained. A successful review is predicated on the Integrated Product Team's determination that the system requirements, approved materiel solution, available product/process technology, and program resources (funding, schedule, staffing, infrastructure, and processes) form a satisfactory basis for proceeding into the EMD phase. The program manager should tailor the review to the technical scope and risk of the system, and address the SRR in the SEP.

Typical SRR success criteria include affirmative answers to the following exit questions:

1. Can the system requirements, as disclosed, satisfy the Initial Capabilities Document or draft Capability Development Document?
2. Are the system requirements sufficiently detailed and understood to enable system functional definition, functional decomposition, test and evaluation?
3. Can the requirements be met given the technology maturation achieved?
4. Is there an approved system performance specification?
5. Are adequate processes and metrics in place for the program to succeed?
6. Have Human Systems Integration and sustainment requirements been reviewed and included in the overall system design?
7. Are the risks known and manageable for development?
8. Is the program schedule executable (technical and/or cost risks)?
9. Is the program properly staffed?
10. Is the program executable within the existing budget?

11. Does the updated cost estimate fit within the existing budget?
12. Is the preliminary Cost Analysis Requirements Description (CARD) consistent with the approved system performance specification?
13. Is the software functionality in the system specification consistent with the software sizing estimates and the resource-loaded schedule?
14. Did the Technology Development phase sufficiently mature all system elements to enable low risk entry into engineering and manufacturing development?
15. Did the Technology Development phase sufficiently mature the critical sustainment enablers technologies required to implement the support strategy and achieve the needed materiel availability?
16. Are the preliminary software development estimates established with effort, schedule, and cost analysis?
17. Have programming languages and architectures, security requirements and operational and support concepts been identified?
18. Have hazards been reviewed and mitigating courses of action been allocated within the overall system design?

The SRR is important in understanding the system performance, cost, and scheduling impacts that the defined requirements will have on the system. This is the last dedicated review of the system requirements, unless an additional SRR is held after the refinement of the system performance constraints during EMD.

The SRR risk assessment checklist is designed as a technical review preparation tool, and should be used as the primary guide for assessing risk during the review. This checklist is available on the Systems Engineering Community of Practice.

4.3.2.4.2.2. System Functional Review (SFR)

The SFR is a multi-disciplined technical review to ensure that the system's functional baseline is established and has a reasonable expectation of satisfying the requirements of the Initial Capabilities Document or draft Capability Development Document within the currently allocated budget and schedule. It completes the process of defining the items or elements below system level. This review assesses the decomposition of the system specification to system functional specifications, ideally derived from use case analysis. A critical component of this review is the development of representative operational use cases for the system. System performance and the anticipated functional requirements for operations maintenance, and sustainment are assigned to sub-systems, hardware, software, or support after detailed analysis of the architecture and the environment in which it will be employed. The SFR determines whether the system's functional definition is fully decomposed to its lower level, and that Integrated Product Teams (IPTs) are prepared to start preliminary design.

The system's lower-level performance requirements are evaluated to determine whether they are fully defined and consistent with the system concept, and whether traceability of lower-level systems requirements to top-level system performance and the CDD is maintained. This activity

results in two major systems engineering products: the final version of the system performance specification and draft version of the performance specifications, which describe the items below system level (item performance specifications). The SFR is the first review that begins to allocate requirements to separated sub-systems and organizational IPTs. As such, it is also the first review where the need for Interface Control Documents becomes necessary to define areas of responsibility and constraints requiring coordination across IPTs. A successful review is predicated on the IPT's determination that the system performance requirements, lower-level performance requirements, and plans for design and development form a satisfactory basis for proceeding into preliminary design.

Completion of the SFR should provide the following:

1. An established system functional baseline with traceability to lower-level performance requirements,
2. An updated risk assessment for the Engineering and Manufacturing Development (EMD) phase,
3. An updated Cost Analysis Requirements Description (CARD) or a CARD-like document based on the system functional baseline,
4. An updated program development schedule including system and software critical path drivers, and
5. A preliminary system level maintenance plan with updates applicable to this phase.

The SFR determines whether the system's lower-level performance requirements are fully defined and consistent with the system concept (including the support concept), and whether lower-level systems requirements trace to top-level system performance and the draft Capability Development Document. A successful SFR is predicated upon the IPT's determination that the system performance requirements, lower-level performance requirements, and plans for design and development form a satisfactory basis for proceeding into preliminary design.

The program manager should tailor the review to the technical scope and risk of the system, and address the SFR in the Systems Engineering Plan (SEP). The SFR is the last review that ensures the system is credible and feasible before more technical design work commences.

Typical SFR success criteria include affirmative answers to the following exit questions:

1. Can the system functional requirements, as disclosed, satisfy the draft Capability Development Document?
2. Are the system functional requirements sufficiently detailed and understood to enable system design to proceed?
3. Are adequate processes and metrics in place for the program to succeed?
4. Are the risks known and manageable for development?
5. Is the program schedule executable (technical/cost risks)?
6. Is the program properly staffed?

7. Is the program with the approved functional baseline executable within the existing budget?
8. Is the updated CARD consistent with the approved functional baseline?
9. Does the updated cost estimate fit within the existing budget?
10. Has the system Functional Baseline been established to enable preliminary design to proceed with proper configuration management?
11. Is the software functionality in the approved functional baseline consistent with the updated software metrics and resource-loaded schedule?
12. Are the supportability requirements to achieve the support strategy included in the performance specifications?
13. Are the program development efforts required to achieve the sustainment key performance parameters and key system attributes and enabler metrics, along with their corresponding schedules, included in the program documentation and Life-cycle Sustainment Plan?
14. Has a draft preliminary Software Requirements Specification been defined, with complete verification requirements?
15. Has an initial software architecture design been defined?
16. Have the system-level hazards been reviewed and mitigating courses of action been identified?

The SFR risk assessment checklist is designed as a technical review preparation tool, and should be used as the primary guide for assessing risk during the review. This checklist is available on the Systems Engineering Community of Practice.

4.3.2.4.2.3. Preliminary Design Review (PDR)

The PDR is a technical assessment establishing the physically allocated baseline to ensure that the system under review has a reasonable expectation of being judged operationally effective and suitable. This review assesses the allocated design documented in subsystem product specifications for each configuration item in the system and ensures that each function, in the functional baseline, has been allocated to one or more system configuration items. The PDR establishes the allocated baseline (hardware, software, human/support systems) and underlying architectures to ensure that the system under review has a reasonable expectation of satisfying the requirements within the currently allocated budget and schedule.

The implementation of the Weapon Systems Acquisition Reform Act of 2009 (see Directive-Type Memorandum (DTM) 09-027 – Implementation of the Weapon Systems Acquisition Reform Act of 2009) directs the following:

a. PDRs before MS B are mandatory for all MDAPs and will be reflected in the Technology Development Strategy (TDS) to be approved by the MDA at MS A. Post-PDR assessments will be conducted in association with MS B preparations and will be formally considered by the MDA at the MS B certification review.

b. The timing of PDRs for other than MDAPs will be approved by the DoD Component MDA when consistent with TDS or Acquisition Strategy objectives. When the PDR is conducted before MS B, a post-PDR assessment will be conducted in association with the MS B review and formally considered by the MDA at the MS B review. If the PDR is conducted after MS B, the MDA will conduct a post-PDR assessment at a time reflected in the approved acquisition strategy.

c. PDR before MS B is now a statutory requirement for MDAPs. The post-PDR assessment will be conducted during the MS B review, and prior to the section 2366b certification by the MDA per title 10, Unites States Code.

This review assesses the allocated design captured in subsystem product specifications for each configuration item (hardware and software) in the system and ensures that each function in the functional baseline has been allocated to one or more system configuration items. Subsystem specifications for hardware and software, along with associated Interface Control Documents, enable detailed design or procurement of subsystems. Configuration items may consist of hardware and software elements, and include items such as structures, avionics/electronics, weapons, crew systems, engines, trainers/training, etc.

Completion of the PDR should provide the following:

1. An established system allocated baseline,
2. An updated risk assessment for Engineering and Manufacturing Development (EMD),
3. An updated Cost Analysis Requirements Description (CARD) or CARD-like document based on the system allocated baseline,
4. An updated program schedule including system and software critical path drivers, and
5. An approved Life-cycle Sustainment Plan updating program sustainment development efforts and schedules.

For complex systems, a PDR may be conducted incrementally for each configuration item. These incremental reviews lead to an overall system level PDR. System level performance is supported by compliance with Interface Control Documents, but not assured. Interface requirements make up each configuration item Allocated Specification. Subsystems that have already completed an incremental PDR may need to be reopened if remaining subsystems cannot achieve desired performance in isolation. If the schedule is being preserved through parallel design decisions, any system deficiencies that lead to reopening design will result in rework and earned value adjustments. It is important to clarify and resolve design conflicts before completing the PDR and entering detailed design.

The PDR evaluates the set of subsystem requirements to determine whether they correctly and completely implement all system requirements allocated to the subsystem. The PDR also determines whether subsystem requirements trace with the system design. At this review, the IPT should review the results of peer reviews of requirements and preliminary design documentation. A successful review is predicated on the IPT's determination that the subsystem requirements,

subsystem preliminary design, results of peer reviews, and plans for development, testing and evaluation form a satisfactory basis for proceeding into detailed design and test procedure development.

The program manager should tailor the review to the technical scope and risk of the system, and address specifics of the PDR in the Systems Engineering Plan (SEP). Typical PDR success criteria include affirmative answers to the following exit questions:

1. Does the status of the technical effort and design indicate operational test and evaluation success (operationally effective and suitable)?
2. Can the preliminary design, as disclosed, satisfy the draft Capability Development Document?
3. Has the system allocated baseline been established and documented to enable detailed design to proceed with proper configuration management?
4. Are adequate processes and metrics in place for the program to succeed?
5. Have sustainment and human integration design factors been reviewed and included, where needed, in the overall system design?
6. Are the risks known and manageable for integrated testing and developmental and operational evaluation?
7. Is the program schedule executable (technical/cost risks)?
8. Is the program properly staffed?
9. Has the program's cost estimate been updated?
10. Is the program executable within the existing budget and with the approved system allocated baseline?
11. Is the preliminary system level design producible within the production budget?
12. Is the updated CARD consistent with the approved allocated baseline?
13. Have the majority of manufacturing processes been defined and characterized?
14. Are initial manufacturing approaches documented?
15. Have producibility assessments of key technologies been completed?
16. Has a production cost model been constructed?
17. Can the industrial base support production of development articles?
18. Have long-lead and key supply chain elements been identified?
19. Can the risks associated with ESOH hazards be mitigated to an acceptable risk level within the existing budget?

With the additional emphasis on PDR, the following exit questions should also be addressed for the system's software component:

1. Has the computer system and software architecture design been established, and have all Computer Software Configuration Items (CSCIs), Computer Software Components (CSCs), and Computer Software Units (CSUs) been defined?
2. Are Software Requirements Specifications and Interface Requirement Specifications, including verification plans, complete and baselined for all CSCs and do they satisfy the system/subsystem functional requirements?

3. Do the Interface Control Documents trace all software interface requirements to the CSCIs and CSUs?
4. Has the computer system and software design/development approach been confirmed through analyses, demonstrations, and prototyping in a relevant environment?
5. Has the preliminary software design been defined and documented?
6. Have software increments been defined and have capabilities been allocated to specific increments?
7. Have software trade studies addressing Commercial-off-the-shelf, reuse, and other software-related issues been completed?
8. Has the software development process been defined in a baselined Software Development Plan and is it reflected in the Integrated Master Plan (IMP) and Integrated Master Schedule (IMS)?
9. Do the software development schedules reflect contractor software processes and IMP/IMS software events for current and future development phases?
10. Have the software development environment and test/integration labs been established with sufficient fidelity and capacity?
11. Have unique software risks been identified/assessed and have mitigation plans been developed/implemented?
12. Have software metrics been defined and reporting process implemented, and are they being actively tracked and assessed?
13. Does the Test and Evaluation Master Plan address all CSCI plans, test facilities, and test plans, including testing required to support incremental approaches (e.g. regression tests)?
14. Is there a life-cycle sustainment plan and does it include software support requirements?
15. Have the software development estimates (i.e. size, effort (cost), and schedule) been updated?
16. Have all required software-related documents been baselined/delivered?

The PDR should be conducted when the allocated baseline has been achieved, allowing detailed design of hardware and software configuration items to proceed. A rule of thumb is that 10 percent to 25 percent of product drawings and associated instructions should be complete, and that 100 percent of all safety-critical component (Critical Safety Items and Critical Application Items) drawings are complete.

The program manager should conduct the PDR when all major design issues have been resolved and work can begin on detailed design. The PDR should address and resolve critical, system-wide issues.

The PDR risk assessment checklist is designed as a technical review preparation tool, and should be used as the primary guide for assessing risk during the review. This checklist is available on the Systems Engineering Community of Practice.

The PDR results are documented in a PDR Report.

4.3.2.4.2.3.1. Preliminary Design Review (PDR) Report

Per DoD Instruction 5000.02, Enclosure 2, paragraph 5.d.(6):

The PDR Report shall be provided to the MDA at Milestone B and include recommended requirements trades based upon an assessment of cost, schedule, and performance risk.

This PDR Report should include the following:

- A description of the systems engineering products that comprised the allocated baseline (to include the preliminary design specifications for configuration items, interface design specifications, and verification plans) and the percentage of the total allocated baseline (design-to packages) completed and subject to this review,
- The names, functional area of responsibility, and organization of all participants in the review, to include the Chair, review board members (if a formal board is convened), program technical representatives, and independent subject matter experts (peer reviewers),
- A summary of the issues identified and actions required to close the review,
- An assessment of risk, by the participants, to commit to full detail Design, and
- An identification of those issues/risks that could result in a breach to the program baseline or substantially impact cost, schedule or performance.

The Director of Systems Engineering shall have access to any DoD component records or data relating to systems engineering and development planning (including classified, unclassified, competition sensitive, and proprietary information) necessary to carry out assigned duties (see Directive-Type Memorandum (DTM) 09-027 – Implementation of the Weapon Systems Acquisition Reform Act of 2009).

The PDR risk assessment checklist is designed as a technical review preparation tool, and should be used as the primary guide for assessing risk during the review. This checklist is available on the Systems Engineering Community of Practice.

4.3.2.4.2.4. Technology Readiness Assessment (TRA)

Per DoD Instruction 5000.02, Enclosure 4 the TRA is a regulatory information requirement for all acquisition programs. The TRA is a systematic, metrics-based process that assesses the maturity of critical technology elements (CTEs), including sustainment drivers. The TRA should be conducted concurrently with other Technical Reviews, specifically the Alternative Systems Review (ASR), System Requirements Review (SRR), or the Production Readiness Review (PRR). If a platform or system depends on specific technologies to meet system operational threshold requirements in development, production, or operation, and if the technology or its application is either new or novel, then that technology is considered a CTE.

The TRA should be considered not as a risk assessment, but as a tool for assessing program risk and the adequacy of technology maturation planning. The TRA scores the current readiness level of selected system elements, using defined Technology Readiness Levels (TRLs). The TRA highlights critical technologies (including critical manufacturing-related technologies) and other potential technology risk areas that require program manager attention. The TRA essentially "draws a line in the sand" on the day of the event for making an assessment of technology readiness for critical technologies integrated at some elemental level. If the system does not meet pre-defined TRL scores, then a CTE maturation plan is identified. This plan explains in detail how the TRL will be reached before the next milestone decision date or relevant decision point. Completion of the TRA should provide the following:

1. A comprehensive review, using an established program Work Breakdown Structure as an outline, of the entire platform or system. This review, using a conceptual or established design, identifies program CTEs,
2. An objective scoring of the level of technological maturity for each CTE by subject matter experts,
3. Maturation plans for achieving an acceptable maturity roadmap for CTEs before critical milestone decision dates, and
4. A final report documenting the findings of the assessment panel.

After the final report is written, it is submitted to the appropriate Service officials and the program manager. Once approved, the report and cover letter are forwarded to the service acquisition official. For Acquisition Category ID or IAM programs, the service acquisition official provides a recommendation to the Director of Defense Research &Engineering (DDR&E) for the Director of Research for final approval. If deemed necessary, the DDR&E can conduct or require an Independent Technology Readiness Assessment in addition to, and totally separate from, the program TRA.

The TRA risk assessment checklist is designed as a technical review preparation tool, and should be used as the primary guide for assessing risk during the review. This checklist is available on the Systems Engineering Community of Practice.

4.3.2.4.2.5. Integrated Baseline Review (IBR)

If an IBR is required in the Technology Development phase, see section 4.3.3.4.1.

4.3.2.5. Outputs of the Systems Engineering Processes in Technology Development

- Live-Fire T&E Waiver request (if appropriate),
- Test and Evaluation Master Plan,
- Risk Assessment,
- Systems Engineering Plan,

- Programmatic Environment, Safety, and Occupational Health Evaluation,
- National Environmental Policy Act Compliance Schedule
- Program Protection Plan,
- Technology Readiness Assessment,
- Validated System Support and Maintenance Objectives and Requirements,
- Initiatives to reduce footprint,
- Inputs to the Integrated Baseline Review,
- Inputs to the Information Support Plan,
- Inputs to the System Threat Assessment Report/System Threat Assessment,
- Inputs to the Capability Development Document,
- Inputs to the Acquisition Strategy,
- Inputs to the Affordability Assessment,
- Inputs to the Cost and Manpower Estimate, and
- System Safety Analyses to include an initial ESOH risk analysis (section 4.4.7.5), completion of Safety Requirements/Criteria Analysis and Preliminary Hazard List for approved materiel solution and initiation of the Preliminary Hazard Analysis and Threat Hazard Assessment.

When a PDR is completed before Milestone B (consistent with the Technology Development Strategy, Test and Evaluation Strategy and Systems Engineering Plan), the following are additional outputs of the Technology Demonstration phase:

- A completed, reviewed, and approved system allocated baseline and
- Preliminary Design Review Report.

4.3.3. Engineering and Manufacturing Development (EMD) Phase

EMD begins at Milestone B, which is normally formal program initiation. This phase is to complete the development of a system or increment of capability, leveraging design considerations; complete full system integration; develop an affordable and executable manufacturing processes, complete system fabrication, test and evaluation. A key emphasis during EMD is to ensure operational supportability with particular attention to minimizing the logistics footprint.

The purposes of EMD are to:

- Develop a system or increment of capability,
- Reduce integration and manufacturing risk,
- Design-in critical supportability aspects to ensure materiel availability with particular attention to reducing the logistics footprint,
- Integrate hardware, software, and human systems,
- Design for producibility,
- Ensure affordability and protection of critical program information, and
- Demonstrate system integration, interoperability, supportability, safety, and utility.

In EMD, the program, the system architecture, and system elements down to the configuration item (hardware and software) level are defined based upon the mature technology suite selected and integrated during Materiel Solution Analysis and Technology Development. During EMD, system design requirements are allocated down to the major subsystem level, and are refined as a result of developmental and operational tests, and iterative systems engineering analyses. The support concept and strategy are refined with detailed design-to requirements determined for the product support package elements.

Effective employment of systems engineering, applied in accordance with a well structured Systems Engineering Plan, and monitored with meaningful metrics and technical reviews, will reduce program risk and identify potential management issues in a timely manner.

4.3.3.1. Purpose of Systems Engineering in Engineering and Manufacturing Development (EMD)

EMD consists of two major, sequential efforts: Integrated System Design and System Capability and Manufacturing Process Demonstration. The EMD systems engineering work effort typically completes the Integrated System Design (including all initial technical reviews not previously completed in Technology Development, and technical reviews intended to occur during EMD) and a System Capability and Manufacturing Process Demonstration. EMD begins when the program manager has an allocated baseline for the system or increment of capability but has not developed or integrated the end item components and subsystems into a fully operational and supportable system. EMD systems engineering work also completes any remaining initial systems design activities not finished during the Technology Development phase (i.e., System Requirements Review, System Functional Review, or Preliminary Design Review).

The primary purpose of systems engineering in EMD is to reduce system-level risk. Through the conduct of systems engineering, the efforts in this phase integrate components and subsystems, and complete the detailed design to meet performance requirements with a producible and sustainable design, and reduce system level risk. EMD typically includes the demonstration of production prototype articles or engineering development models. When the necessary industrial capabilities are available, the system satisfies approved requirements, and the system meets or exceeds exit criteria and Milestone C entrance requirements, the EMD effort may end. Key to the systems engineering in the EMD phase is acceptable performance in integrated test, developmental evaluation and operational assessments, and the use of modeling and simulation in test and evaluation and the demonstration of satisfactory system integration.

4.3.3.2. Inputs to the Systems Engineering Processes in Engineering and Manufacturing Development (EMD)

When a Preliminary Design Review (PDR) has been completed before Milestone B (consistent with the Technology Development Strategy, Test and Evaluation Strategy and Systems Engineering Plan), the following are inputs to the systems engineering processes in EMD:

- A completed, reviewed, and approved system allocated baseline,
- A PDR Report,
- System Performance Specification,
- Exit criteria for the EMD phase,
- Validated System Support and Maintenance Objectives and Requirements,
- Acquisition Program Baseline,
- Capability Development Document,
- Systems Engineering Plan,
- Information Support Plan,
- Test and Evaluation Master Plan,
- Programmatic Environment, Safety, and Occupational Health Evaluation,
- Life-cycle Sustainment Plan,
- Inputs for the Program Protection Plan (see also section 8.4.6),
- Inputs for the System Threat Assessment Report/System Threat Assessment, and
- System Safety Analyses to include initial ESOH risk analysis (section 4.4.7.5), completion of Safety Requirements Criteria Analysis and Preliminary Hazard List for approved materiel solution and initiation of the Preliminary Hazard Analysis and Threat Hazard Assessment.

4.3.3.3. Key Systems Engineering Activities During Engineering and Manufacturing Development (EMD)

Figure 4.3.3.3.F1 identifies the systems engineering-related steps during the EMD phase.

Note: Given the iterative and recursive nature of systems engineering, the sequence of activities in figure 4.3.3.3.F1 (displayed in the highlighted rectangles) is in their order of completion, vice the order of commencement. The activities can be started in any order and often run in parallel, but they should be completed in the order shown. Paragraphs below contain additional detail on each step.

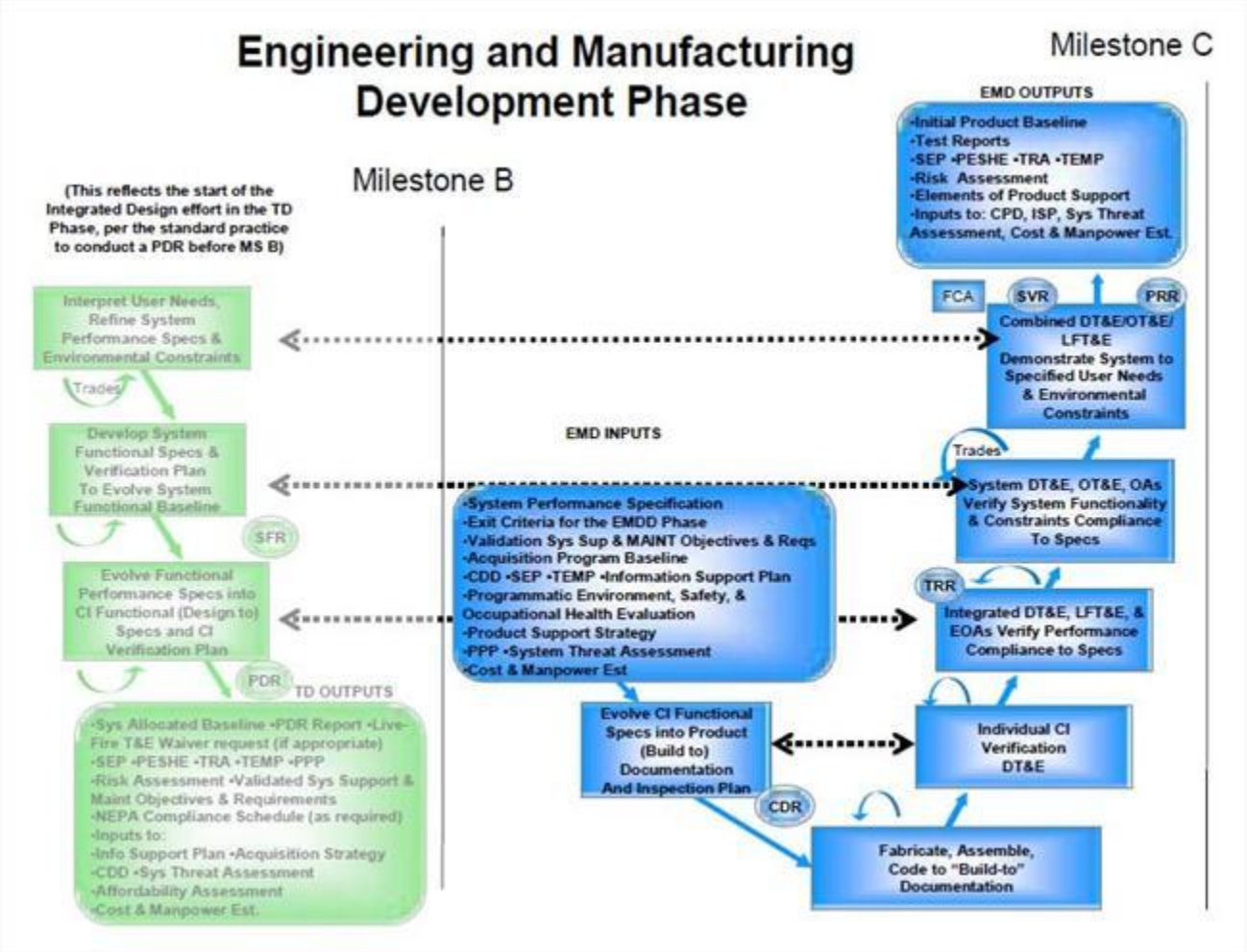


Figure 4.3.3.3.F1. Systems engineering-related steps during the System Design effort of Engineering and Manufacturing Development

4.3.3.3.1. Evolve Configuration Item Design Specifications into System Product Baseline

This step finalizes the detailed design of the system. The design should include all hardware and software components. The engineers should complete drawings and other "build-to" documentation for the components (i.e., fabricating hardware components or coding the software element) and plan for integration, testing and evaluation. These build-to documents may include manufacturing drawings, materiel specifications, software design (code-to) specifications, and associated verification plans. Matured technologies and existing designs (re-use or Commercial-off-the-shelf) are integrated into the detailed design of the configuration items and overall system. Sustainment; Environment, Safety, and Occupational Health; and other life-cycle and/or environmental considerations that affect the component level of the system should be part of the decision making and trade studies that occur at this level of design. The program manager should

ensure the program team continually assesses cost, schedule, and performance against the detailed design. Additional analyses at this step include Level of Repair Analyses and Maintenance Task Analyses. Analysts should estimate the projected system reliability from demonstrated reliability rates.

A Critical Design Review (CDR) is normally conducted to establish the product baseline for each configuration item culminating in a system-level CDR that approves the product baseline for the overall system. The end product of the CDR is a product baseline and the technical basis for the CDR Report to the MDA. A high percentage of manufacturing drawings should have been validated and approved prior to any CDR.

4.3.3.3.2. Fabricate, Assemble, Code to Product Baseline

This step involves fabricating hardware components and coding software components; acquiring all other components, including commercial items, being bought or reused, and then assembling the components according to the integration, test, and evaluation planning. At this point, all the system, subsystem, and component design requirements should have been developed. The program manager should manage the design requirements and plan for corrective action for any discovered hardware and software deficiencies. If any technology is not mature enough for use in the current increment system, an off-ramp technology to mitigate risk should be identified. The program manager should integrate, test and evaluate an alternative, mature, technology in its place. The program manager should defer immature technology to the next increment of the system. The program manager should ensure the program team continually assesses cost, schedule, and performance against the evolving product baseline.

This step will usually result in prototypes and engineering development models, and should include developmental testing to support the Critical Design Review.

4.3.3.3.3. Developmental Evaluation Verifies Individual Configuration Items

This step calls for the demonstration (according to the verification and validation plans) of the physical, electrical, software, and other characteristics of the components to be integrated. Unit testing and evaluation of hardware and independent verification and validation of software are initiated. Special attention should be placed on the integration and testing of commercial components. Components and any assemblies of them are tested to determine if they meet their requirements and function in the environment of their intended use. Developmental test and evaluation is conducted on the configuration items (hardware and software) to assess technical progress against critical technical parameters. Monitoring of risk, cost, and schedule continue and design issues that arise as a result of the integration, verification, or validation processes should feed back into the design solution process for refinement of the design. Early component level test may not require the same level of review as the final system level tests.

4.3.3.3.4. Integrated Test for Developmental and Live Fire Evaluation, and Operational Assessments verify Performance Compliance to Specifications

This step calls for the verification of subsystem hardware and software performance against their defined subsystem design requirements. Subsystem hardware and software are demonstrated in their intended environment. Developmental evaluation, operational assessments, and integrated tests (combined developmental and operational) are conducted at the subsystem level, and risk, cost, and schedule continue to be monitored.

System Integration Laboratories (SILs) are generally used to integrate subsystems, and in testing the full up system. The SIL should have been developed concurrently with the system. The SIL may be networked with other Laboratories and simulation facilities to assess interoperability with other emerging and legacy systems. If the SIL is to be used for test and evaluation, it needs to be verified and accredited in accordance with a verification and validation plan.

The Test Readiness Review (TRR) occurs after this activity. The program manager determines the 'formality' and scope of the Test Readiness Review for each assembly or subsystem.

The program manager also ensures the conduct of the Functional Configuration Audit to verify that the actual performance of the configuration items (hardware and software) meets specification requirements.

4.3.3.3.5. Integrated Test for Developmental and Live Fire Evaluation, and Operational Assessments verify System Functionality and Constraints Compliance to Specifications

This step calls for the integration of the subsystems into the defined system and demonstrates the integrated system under its operational environment constraints. It verifies that the system meets performance and functionality requirements, and validates the use of the system in its intended environment. This step includes integrated test and developmental evaluation, any live fire evaluation, and operational assessments on the integrated system (see section 9.0.2). All integration and interface issues should be resolved. Risks are monitored and analyzed as they pertain to the cost, schedule, and performance of the integrated system.

4.3.3.3.6. Integrated Test, Developmental Evaluation, Operational Assessments, and Live Fire Evaluation Demonstrate System to Specified User Needs and Environmental Constraints

In this step, the integrated system is verified and validated against the specified operational systems requirements within the required operational environment(s) to ensure the system can satisfy operational requirements. Test environments and scenarios should be defined, and cost,

schedule, and performance considerations should be continually addressed. This involves interoperability and interfaces for the system within any system of systems in which it operates. Any interface and interoperability issues for the system should be resolved for the system to achieve its interoperability certification in the next phase. Operational supportability should be confirmed at this time to verify and validate that the product support package is operationally suitable and effective. This should include verifying that the key sustainment enabling technologies embedded into design are mature enough support the Life-cycle Sustainment Plan. In preparation for the Production Readiness Review, this step should confirm that the manufacturing processes are under control and that there are no significant manufacturing risks. Technical risk should be addressed, characterized, and mitigated.

4.3.3.4. Technical Reviews During Engineering and Manufacturing Development (EMD)

4.3.3.4. Technical Reviews During Engineering and Manufacturing Development (EMD)

Any of the initial systems design steps supporting Integrated System Design and listed in table 4.3.3.4.T1 that are not completed during Technology Development should be completed upon entry into EMD.

Technical Reviews and Reports in Technology Development
System Requirements Review
System Functional Review
System Preliminary Design Review

Preliminary Design Review (PDR) Report

Table 4.4.3.4.T1. Integrated System Design Reviews and Report

Program systems engineering efforts continue after the establishment of an allocated baseline representing the initial systems design, completion of the Detail System Design, and completion of a System Capability and Manufacturing Process Demonstration. The remaining technical reviews and assessments are described in Sections 4.3.3.4.1 through 4.3.3.4.8 and identified in table 4.3.3.4.T2.

Technical Reviews and Reports in EMD
Integrated Baseline Review (IBR)
Critical Design Review
Test Readiness Review
Flight Readiness Review (FRR)
System Verification Review (SVR)
Functional Configuration Audit
Production Readiness Review
Technology Readiness Assessment

Table 4.4.3.4.T2. Technical Reviews and Reports in EMD

4.3.3.4.1. Integrated Baseline Review (IBR)

An Integrated Baseline Review (IBR) is a joint assessment conducted by the government program manager and the contractor to establish the Performance Measurement Baseline (PMB). The IBR is not a one-time event. IBRs should be scheduled as early as practicable and the timing of the IBRs should take into consideration the contract period of performance. The process should be initiated not later than 180 calendar days (6 months) after: (1) contract award, (2) the exercise of significant contract options, and (3) the incorporation of major modifications.

Program managers should use the IBR throughout the program when Earned Value Management is required. This review has a business focus, but should include the important technical considerations discussed below.

The process is composed of four steps:

1. The program manager's assessment of their understanding of the risks,

2. Preparation for an IBR,
3. Execution of the IBR, and
4. Management processes.

The key step in the process is execution of the IBR. The IBR establishes a mutual understanding of the project PMB. This understanding provides for an agreement on a plan of action to evaluate the risks inherent in the PMB and the management processes that operate during program execution. The PMB should be placed under configuration control with changes only upon mutual agreement of the government and contractor.

Completion of the review should result in the assessment of risk within the program measurement baseline and the degree to which the following have been established:

1. Technical scope of work is fully included and is consistent with authorizing documents,
2. Key project schedule milestones are identified and supporting schedules reflect a logical flow to accomplish the work,
3. Resources (budgets, facilities, infrastructure, personnel, skills, etc.) are available and are adequate for the assigned tasks,
4. Tasks are planned and can be measured objectively relative to the technical progress,
5. Rationales underlying the PMB are reasonable, and
6. Management processes support successful execution of the project.

Section 11.3.1.3 describes the IBR. The Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, in cooperation with industry, has also prepared The Program Managers' Guide to the Integrated Baseline Review Process. Also, see the DoD Earned Value Management Implementation Guide for additional guidance on IBRs.

The IBR Risk Assessment Checklist is designed as a technical review preparation tool, and should be used as the primary guide for assessing risk during the review. This checklist is available on the Systems Engineering Community of Practice.

4.3.3.4.2. Critical Design Review (CDR)

The CDR is a key point within the Engineering and Manufacturing Development (EMD) phase. The CDR is a multi-disciplined technical review establishing the initial product baseline to ensure that the system under review has a reasonable expectation of satisfying the requirements of the Capability Development Document within the currently allocated budget and schedule. Incremental CDRs are held for each Configuration Item culminating with a system level CDR. This review assesses the final design as captured in product specifications for each Configuration Item in the system and ensures that each product specification has been captured in detailed design documentation. Configuration Items may consist of hardware and software elements, and include items such as airframe/hull, avionics, weapons, crew systems, engines, trainers/training, support equipment, etc. Product specifications for hardware enable the fabrication of configuration items, and include production drawings. Product specifications for software enable

coding of the Computer Software Configuration Item. The CDR evaluates the proposed Baseline ("Build To" documentation) to determine if the system design documentation (Initial Product Baseline, including Item Detail Specs, Material Specs, Process Specs) is satisfactory to start initial manufacturing.

The CDR brings closure to technical risk mitigation and alternate design paths in detailed system design. Once the product baseline is established, opportunities to improve performance or reduce life-cycle costs are severely limited. Changes to support equipment, training requirements, logistics and supply elements, interoperability, and performance can only be accomplished through a formal Engineering Change Proposal. All technical risk should be reduced to acceptable levels and remaining program execution risk resulting from resource or schedule shortfalls should be addressed quickly or it will jeopardize program success.

Completion of the CDR should provide the following:

1. An established system initial product baseline,
2. An updated risk assessment for EMD,
3. An updated CARD (or CARD-like document) based on the system product baseline,
4. An updated program development schedule including fabrication, test and evaluation, and software coding, critical path drivers, and
5. An approved Life-cycle Sustainment Plan updating program sustainment development efforts and schedules based on current budgets, test evaluation results and firm supportability design features.

For complex systems, a CDR may be conducted for each subsystem and logistics element. These incremental reviews lead to an overall system CDR. Incremental design reviews are usually defined at Interface Control Document boundaries. System level performance is supported by compliance with Interface Control Documents, but not assured. When incremental reviews have been conducted, additional risk is introduced until the overall system CDR establishes the complete system product baseline. Each incremental CDR closes a functional or physical area of design to modification regardless of when it is held. This completed area of design may need to be reopened if open areas cannot achieve desired performance in isolation. If the schedule is being preserved through parallel design and build decisions, any system deficiencies that lead to reopening design will result in rework and possible material scrap.

At CDR, the EMD process results in a detailed product baseline for the system, hardware, software, support equipment, training systems, system integration laboratory, and technical data. The subsystem detailed designs and logistics elements are evaluated to determine whether they correctly and completely implement all allocated system requirements, and whether the CDD traceability to final system detail design is maintained. Any changes during EMD are incorporated, and the CDD evolves to the Capability Production Document (CPD) required at Milestone C. The overall system level CDR is not only approval of the system product baseline, but also approval of the product baselines for maintainability, supportability, and logistics elements. A successful review is predicated on the review chairperson's determination that the

subsystem requirements, subsystem detail design, results of peer reviews, and plans for test and evaluation form a satisfactory basis for proceeding into system fabrication, demonstration and test.

The CDR chairperson should tailor the review to the technical scope and risk of the system, and address specifics of the CDR in the Systems Engineering Plan.

Typical CDR success criteria include affirmative answers to the following exit questions:

1. Does the status of the technical effort and design indicate operational test and evaluation success (operationally effective and suitable)?
2. Does the detailed design (hardware and software) including interface descriptions completed, as disclosed, satisfy the Capabilities Development Document or any available draft Capability Production Document?
3. Has the system product baseline been established and documented to enable hardware fabrication and software coding to proceed with proper configuration management?
4. Has the detailed design satisfied sustainment and Human Systems Integration requirements?
5. Are adequate processes and metrics in place for the program to succeed?
6. Are the risks known and manageable for testing in support of developmental and operational evaluation objectives?
7. Is the program schedule executable (technical/cost risks)?
8. Is the program properly staffed?
9. Is the program executable with the existing budget and the approved product baseline?
10. Is the detailed design producible within the production budget?
11. Is the updated Cost Analysis Requirements Description (CARD) consistent with the approved product baseline?
12. Are all Critical Safety Items and Critical Application Items identified?
13. Does the updated cost estimate fit within the existing budget?
14. Is the software functionality in the approved product baseline consistent with the updated software metrics and resource-loaded schedule?
15. Have key product characteristics having the most impact on system performance, assembly, cost, reliability, and sustainment or safety been identified?
16. Have the critical manufacturing processes that affect the key characteristics been identified and their capability to meet design tolerances determined?
17. Have process control plans been developed for critical manufacturing processes?
18. Have manufacturing processes been demonstrated in a production representative environment?
19. Are detailed trade studies and system producibility assessments underway?
20. Are materials and tooling available to meet pilot line schedule?
21. Has the system production cost model been updated, allocated to subsystem level, and tracked against targets?
22. Are long lead procurement plans in place and has the supply chain been assessed?
23. Are the ESOH residual risks known and manageable?

The CDR should be conducted when the product baseline has been achieved, allowing fabrication of hardware and coding of software deliverables to proceed. A rule of thumb is that 75 percent to 90 percent of (manufacturing quality) product drawings, software design specification(s) and associated instructions should be complete, and that 100 percent of all safety-critical component (Critical Safety Items and Critical Application Items) drawings are complete. Many programs use drawing (Computer Added Design models) releases as a metric for measuring design completion.

The CDR is followed by a Milestone Decision Authority Post-CDR Assessment (for Acquisition Category I programs) to ensure that the system under review can proceed into system fabrication, demonstration, and test, and can meet the stated performance requirements within cost (program budget), schedule (program schedule), risk, and other system constraints.

CDR Report

DoD Instruction 5000.02, Enclosure 2, paragraph 6.c.(6)(c)1, directs the reporting of the results from the completion of the CDR per the following extract:

The PM shall provide a Post-CDR Report to the MDA that provides an overall assessment of design maturity and a summary of the system-level CDR results which shall include, but not be limited to:

- The names, organizations, and areas of expertise of independent subject matter expert participants and CDR chair,
- A description of the product baseline for the system and the percentage of build-to packages completed for this baseline,
- A summary of the issues and actions identified at the review together with their closure plans,
- An assessment of risk by the participants against the exit criteria for the EMD phase, and
- Identification of those issues/risks that could result in a breach to the program baseline or substantively impact cost, schedule or performance.

The Director of Systems Engineering shall have access to any DoD component records or data relating to systems engineering and development planning (including classified, unclassified, competition sensitive, and proprietary information) necessary to carry out assigned duties (see Directive-Type Memorandum (DTM) 09-027 – Implementation of the Weapon Systems Acquisition Reform Act of 2009).

The CDR risk assessment checklist is designed as a technical review preparation tool, and should be used as the primary guide for assessing risk during the review. This checklist is available on the Systems Engineering Community of Practice.

4.3.3.4.3. Test Readiness Review (TRR)

The TRR is a multi-disciplined technical review designed to ensure that the subsystem or system under review is ready to proceed into formal test. The TRR assesses test objectives, test methods and procedures, scope of tests, and safety and confirms that required test resources have been properly identified and coordinated to support planned tests. The TRR verifies the traceability of planned tests to program requirements and user needs. It determines the completeness of test procedures and their compliance with test plans and descriptions. The TRR also assesses the system under review for development maturity, cost/ schedule effectiveness, and risk to determine readiness to proceed to formal testing. In addition to adequate planning and management, to be effective the program manager should follow-up with the outcomes of the TRR.

Test and evaluation is an integral part of the systems engineering processes of verification and validation. Test and evaluation should permeate the entire life cycle of an acquisition program and is also an important tool to identify and control risk.

This discussion principally addresses the TRR to support the readiness for a system to proceed into system level test. However, the program manager could use the TRR process to support all tests in all phases of an acquisition program, including testing within a system of systems context. A robust integrated test program should enhance the program manager's ability to identify and manage risk. The program managers and the test and evaluation working-level Integrated Product Team (IPT) (T&E WIPT) should tailor any TRR to the specific acquisition phase, the specific planned tests, and the identified level of risk within the program. The scope of the review is directly related to the risk level associated with performing the planned tests and the importance of the test evaluation results to overall program success. The program manager should address the scope of the TRR(s) in the Systems Engineering Plan.

The level of specific risk and associated risk level will vary as a system proceeds from component level, to system level, to systems of systems level testing. Early component level tests may not require the same level of review as the final system level tests. Sound judgment should dictate the scope of a specific test or series of tests.

Readiness to convene a TRR is predicated on the program manager's and T&E WIPT's determination that preliminary, functional, and pre-qualification test evaluation results form a satisfactory basis for proceeding with a TRR and subsequent initiation of formal, system-level test. As a practical matter, the program manager should carefully plan and properly resource test events. Regardless of stage of development or the level of the testing (component, subsystem, or system), the basic tenets of this discussion about the TRR should apply.

The TRR should answer the following questions:

1. Why are we testing? What is the purpose of the planned test? Does the planned test verify a requirement that is directly traceable back to a system specification or other program requirement?

2. What are we testing (subsystem, system, system of systems, other)? Is the configuration of the system under test sufficiently mature, defined, and representative to accomplish planned test objectives and or support defined program objectives?
3. Are we ready to begin testing? Have all planned preliminary, informal, functional, unit level, subsystem, system, and qualification tests been conducted, and are the results satisfactory?
4. What is the expected result and how can/do the test evaluation results affect the program?
5. Is the planned test properly resourced (people, test article or articles, facilities, data systems, support equipment, logistics, etc.)?
6. What are the risks associated with the tests and how are they being mitigated?
7. What are the hazards and ESOH risks associated with the specific testing?
8. Have the necessary "Safety Releases" from the Program Manager (PM) been provided to developmental and operational testers prior to any test using personnel?
9. What is the fall-back plan should a technical issue or potential showstopper arise during testing?

Typical TRR success criteria include the following:

1. Completed and approved test plans for the system under test,
2. Completed identification and coordination of required test resources,
3. The judgment that previous component, subsystem, and system test results form a satisfactory basis for proceeding into planned tests, and
4. Identified risk level acceptable to the program leadership.

Test and evaluation is critical to evaluating the system. The TRR ensures the testing to be conducted properly evaluates the system and the system is ready to be tested.

The TRR risk assessment checklist is designed as a technical review preparation tool, and should be used as the primary guide for assessing risk during the review. This checklist is available on the Systems Engineering Community of Practice.

4.3.3.4.4. Flight Readiness Review (FRR)

The FRR is a sub-set of the Test Readiness Review, and is applicable only to aviation programs. It assesses the readiness to initiate and conduct flight tests or flight operations. Typically, FRR approval requires the aviation system to be under configuration management, a flight clearance issued by the technical authority, the flight test plan(s) approved, and discrepancy tracking and risk assessment processes in place.

The FRR risk assessment checklist is designed as a technical review preparation tool, and should be used as the primary guide for assessing risk during the review. This checklist is available on the Systems Engineering Community of Practice.

4.3.3.4.5. System Verification Review (SVR)

The SVR is a multi-disciplined product and process assessment to ensure the system under review can proceed into Low-Rate Initial Production and full-rate production within cost (program budget), schedule (program schedule), risk, and other system constraints. Generally this review is an audit trail from the System Functional Review. It assesses the system functionality, and determines if it meets the functional requirements (derived from the Capability Development Document and draft Capability Production Document) documented in the functional baseline. The SVR establishes and verifies final product performance. It provides inputs to the Capability Production Document. The SVR is often conducted concurrently with the Production Readiness Review. A Functional Configuration Audit may also be conducted concurrently with the SVR, if desired.

Typical SVR success criteria include affirmative answers to the following exit questions:

1. Does the status of the technical effort and system indicate operational test success (operationally effective and suitable)?
2. Can the system, as it exists, satisfy the Capabilities Development Document/draft Capability Production Document?
3. Are adequate processes and metrics in place for the program to succeed?
4. Are the risks known and manageable?
5. Is the program schedule executable within the anticipated cost and technical risks?
6. Are the system requirements understood to the level appropriate for this review?
7. Is the program properly staffed?
8. Is the program's non-recurring engineering requirement executable with the existing budget?
9. Is the system producible within the production budget?

The SVR risk assessment checklist is designed as a technical review preparation tool, and should be used as the primary guide for assessing risk during the review. This checklist is available on the Systems Engineering Community of Practice.

4.3.3.4.6. Functional Configuration Audit (FCA)

A FCA may also be conducted concurrently with the System Verification Review. The FCA is the formal examination of the as tested characteristics of a configuration item (hardware and software) with the objective of verifying that actual performance complies with design and interface requirements in the functional baseline. It is essentially a review of the configuration item's test/analysis data, including software unit test results, to validate the intended function or performance stated in its specification is met. For the overall system, this would be the system performance specification. For large systems, audits may be conducted on lower level configuration items for specific functional areas and address non-adjudicated discrepancies as part of the FCA for the entire system. A successful FCA typically demonstrates that Engineering

and Manufacturing Development product is sufficiently mature for entrance into Low-Rate Initial Production.

4.3.3.4.7. Production Readiness Review (PRR)

The PRR examines a program to determine if the design is ready for production and if the prime contractor and major subcontractors have accomplished adequate production planning without incurring unacceptable risks that will breach thresholds of schedule, performance, cost, or other established criteria. The review examines risk; it determines if production or production preparations identify unacceptable risks that might breach thresholds of schedule, performance, cost, or other established criteria. The review evaluates the full, production-configured system to determine if it correctly and completely implements all system requirements. The review determines whether the traceability of final system requirements to the final production system is maintained.

At this review, the Integrated Product Team (IPT) should review the readiness of the manufacturing processes, the quality management system, and the production planning (i.e., facilities, tooling and test equipment capacity, personnel development and certification, process documentation, inventory management, supplier management, etc.). A successful review is predicated on the IPT's determination that the system requirements are fully met in the final production configuration, and that production capability forms a satisfactory basis for proceeding into Low-Rate Initial Production (LRIP) and Full-rate production.

The program manager should convene a PRR of the prime contractor and major subcontractors, as applicable. The PRR(s) should be conducted in an iterative fashion, concurrently with other technical reviews, such as the CDR, during the Engineering and Manufacturing Development (EMD) phase. Periodic production readiness assessments should be conducted during System Capability and Manufacturing Process Demonstration to identify and mitigate risks as the design progresses. The 'final' PRR should occur at the completion of the EMD phase and the start of the Production and Deployment phase. The final PRR should assess the manufacturing and quality risk as the program proceeds into LRIP and full-rate production.

The program manager should tailor the PRR to the technical scope and risks associated with the system, and provide the details in the Systems Engineering Plan.

Typical PRR success criteria include affirmative answers to the following exit questions:

1. Has the system product baseline been established and documented to enable hardware fabrication and software coding to proceed with proper configuration management?
2. Are adequate processes and metrics in place for the program to succeed?
3. Are the risks known and manageable?
4. Is the program schedule executable (technical/cost risks)?
5. Is the program properly staffed?
6. Are all technologies mature enough for production?

7. Is the detailed design producible within the production budget?
8. Are the production facilities ready and required workers trained?
9. Is detail design complete and stable enough to enter low rate production?
10. Is the supply chain established and stable with materials available to meet planned low rate production?
11. Have manufacturing processes been demonstrated and proven in a pilot line environment?
12. Have all producibility trade studies and risk assessments been completed?
13. Is the production cost model based upon the stable detailed design and been validated?
14. Are the ESOH residual risks known and manageable?

A follow-on, tailored, PRR may be appropriate in the Production and Deployment phase for the prime contractor and major subcontractors if:

1. Changes from the EMD phase and during the production stage of the design, in either materials or manufacturing processes, occur,
2. Production start-up or re-start occurs after a significant shutdown period,
3. Production start-up with a new contractor, or
4. Relocation of a manufacturing site.

The PRR risk assessment checklist is designed as a technical review preparation tool, and should be used as the primary guide for assessing risk during the review. This checklist is available on the Systems Engineering Community of Practice.

4.3.3.4.8. Technology Readiness Assessment (TRA)

The program manager should normally conduct a second TRA prior to Milestone C. The TRA may be held concurrently with other technical reviews, specifically System Verification Review, or Production Readiness Review. Completion of this TRA should provide:

1. An evaluation of system technology maturity based on the Work Breakdown Structure,
2. An objective scoring of the level of technological maturity, and
3. Mitigation plans for achieving acceptable maturity prior to milestone decision dates.

The TRA risk assessment checklist is designed as a technical review preparation tool, and should be used as the primary guide for assessing risk during the review. This checklist is available on the Systems Engineering Community of Practice.

4.3.3.5. Outputs of the Systems Engineering Processes in Engineering and Manufacturing Development

- Product Baseline,
- Test Reports,

- Test and Evaluation Master Plan,
- Product Support Element Requirements,
- Risk Assessment (see also section 8.4.4.1),
- Systems Engineering Plan,
- Technology Readiness Assessment,
- Programmatic Environment, Safety, and Occupational Health Evaluation,
- Inputs to the Capability Production Document,
- Inputs to System Threat Assessment Report/System Threat Assessment,
- Information Support Plan,
- Inputs to Cost and Manpower Estimate, and
- System Safety Analyses to include updated ESOH risk analysis (section 4.4.7.5), completion of Preliminary Hazard Analysis, Safety Requirements/Criteria Analysis, and Operating & Support Hazard Analysis; finalize the System Safety Hazard Analyses, System Hazard Analysis, and Threat Hazard Assessment; and, identify Environment, Safety, and Occupational Health requirements, constraints, footprint, and attributes.

4.3.4. Production and Deployment Phase

The Production and Deployment Phase commences at Milestone C. During the Production and Deployment phase, the system should achieve operational capability that satisfies mission needs.

Two work efforts, separated by the Full-Rate Production Decision Review, comprise the Production and Deployment Phase: Low-Rate Initial Production and Full-Rate Production and Deployment.

Effective employment of systems engineering, applied in accordance with a well structured Systems Engineering Plan, and monitored with meaningful technical reviews, will reduce program risk and identify potential management issues in a timely manner.

4.3.4.1. Purpose of Systems Engineering in Production and Deployment

As the integrated components develop into a system, the test and evaluation processes frequently reveal issues that require improvements or redesign. As the testing environment more closely approaches that of the users' needs, the required improvements might be complex and/or subtle. The initial manufacturing process may also reveal issues that were not anticipated. It may be discovered that changing the product somewhat may provide enhancements in the manufacturing or other supporting processes. Low-Rate Initial Production should result in completion of manufacturing development. The systems engineering effort in Full-Rate Production and Deployment delivers the fully funded quantity of systems and supporting materiel and services for the program or increment. During this effort, units attain Initial Operational Capability.

4.3.4.2. Inputs to the Systems Engineering Processes in Production

and Deployment

- Evaluation results from test,
- Exit criteria for the Production and Deployment Phase,
- Entrance criteria for the Operations and Support Phase,
- Acquisition Program Baseline,
- Capability Development Document and Capability Production Document,
- Systems Engineering Plan,
- Test and Evaluation Master Plan,
- Programmatic Environment, Safety, and Occupational Health Evaluation,
- Product Support Element Requirements, and
- System Safety Analyses to include updated ESOH risk analysis (section 4.4.7.5), update to Safety Requirements Criteria Analysis, System Safety Hazard Analysis, System Hazard Analysis, and Operating &Support Hazard Analysis.

4.3.4.4. Technical Reviews During Production and Deployment

4.3.4.4.1. Integrated Baseline Review (IBR)

The program manager may convene an additional IBR to support the Low-Rate Initial Production contract. The link above will discuss the systems engineering considerations associated with an IBR. Section 11.3.1.3 describes an IBR in more detail. The Program Managers' Guide to the Integrated Baseline Review Process defines the purpose, goals, and objectives of an IBR.

Completion of IBR at this stage of the life cycle should result in the assessment of risk and the degree to which the six criteria described in Section 4.3.3.4.1 are met.

The IBR risk assessment checklist is designed as a technical review preparation tool, and should be used as the primary guide for assessing risk during the review. This checklist is available on the Systems Engineering Community of Practice.

4.3.4.4.2. Operational Test Readiness Review (OTRR)

The OTRR is a multi-disciplined product and process assessment to ensure that the system can proceed into Initial Operational Test and Evaluation with a high probability of success, and that

the system is effective and suitable for service introduction. The Full-Rate Production Decision may hinge on this successful determination. The understanding of available system performance in the operational environment to meet the Capability Production Document is important to the OTRR. Consequently, it is important the test addresses and verifies system reliability, maintainability, and supportability performance and determines if the hazards and ESOH residual risks are manageable within the planned testing operations. The OTRR is complete when the Service Acquisition Executive evaluates and determines materiel system readiness for Initial Operational Test and Evaluation.

The OTRR risk assessment checklist is designed as a technical review preparation tool, and should be used as the primary guide for assessing risk during the review. This checklist is available on the Systems Engineering Community of Practice.

4.3.4.4.3. Physical Configuration Audit (PCA)

The PCA is conducted around the time of the Full-Rate Production Decision. The PCA examines the actual configuration of an item being produced. It verifies that the related design documentation matches the item as specified in the contract. In addition to the standard practice of assuring product verification, the PCA confirms that the manufacturing processes, quality control system, measurement and test equipment, and training are adequately planned, tracked, and controlled. The PCA validates many of the supporting processes used by the contractor in the production of the item and verifies other elements of the item that may have been impacted/redesigned after completion of the System Verification Review. A PCA is normally conducted when the government plans to control the detail design of the item it is acquiring via the Technical Data Package. When the government does not plan to exercise such control or purchase the item's Technical Data Package (e.g., performance based procurement), the contractor should conduct an internal PCA to define the starting point for controlling the detail design of the item and establishing a product baseline. The PCA is complete when the design and manufacturing documentation match the item as specified in the contract. If the PCA was not conducted before the Full-Rate Production Decision, it should be performed as soon as production systems are available.

The PCA risk assessment checklist is designed as a technical review preparation tool, and should be used as the primary guide for assessing risk during the review. This checklist is available on the Systems Engineering Community of Practice.

4.3.4.5. Outputs of the Systems Engineering Processes in Production and Deployment

- Updated Product Baseline,
- Evaluation results from test,
- Test and Evaluation Master Plan,
- Risk Assessment,

- Life-cycle Sustainment Plan,
- Programmatic Environment, Safety, and Occupational Health Evaluation,
- National Environmental Policy Act (NEPA) Compliance Schedule,
- Systems Engineering Plan,
- Inputs to Cost and Manpower Estimate, and
- System Safety Analyses to include finalizing hazard analyses and associated ESOH risk analysis (section 4.4.7.5).

4.3.4.3. Key Systems Engineering Activities During Production and Deployment

4.3.4.3. Key Systems Engineering Activities During Production and Deployment

Figure 4.3.4.3.F1 illustrates the steps during the Production and Deployment phase. Some activities and reports are shown outside of the systems engineering V-shaped model that was used in describing the other phases. Note: Given the iterative and recursive nature of systems engineering, the sequence of activities (displayed in the highlighted rectangles) is in their order of completion, vice the order of commencement. The activities can be started in any order and often run in parallel, but they should be completed in the order shown. The following paragraphs, 4.3.4.3.1. through 4.3.4.3.3, contain further detail about each step. The Integrated Baseline Review, Operational Test Readiness Review, and Physical Configuration Audit are discussed after that.

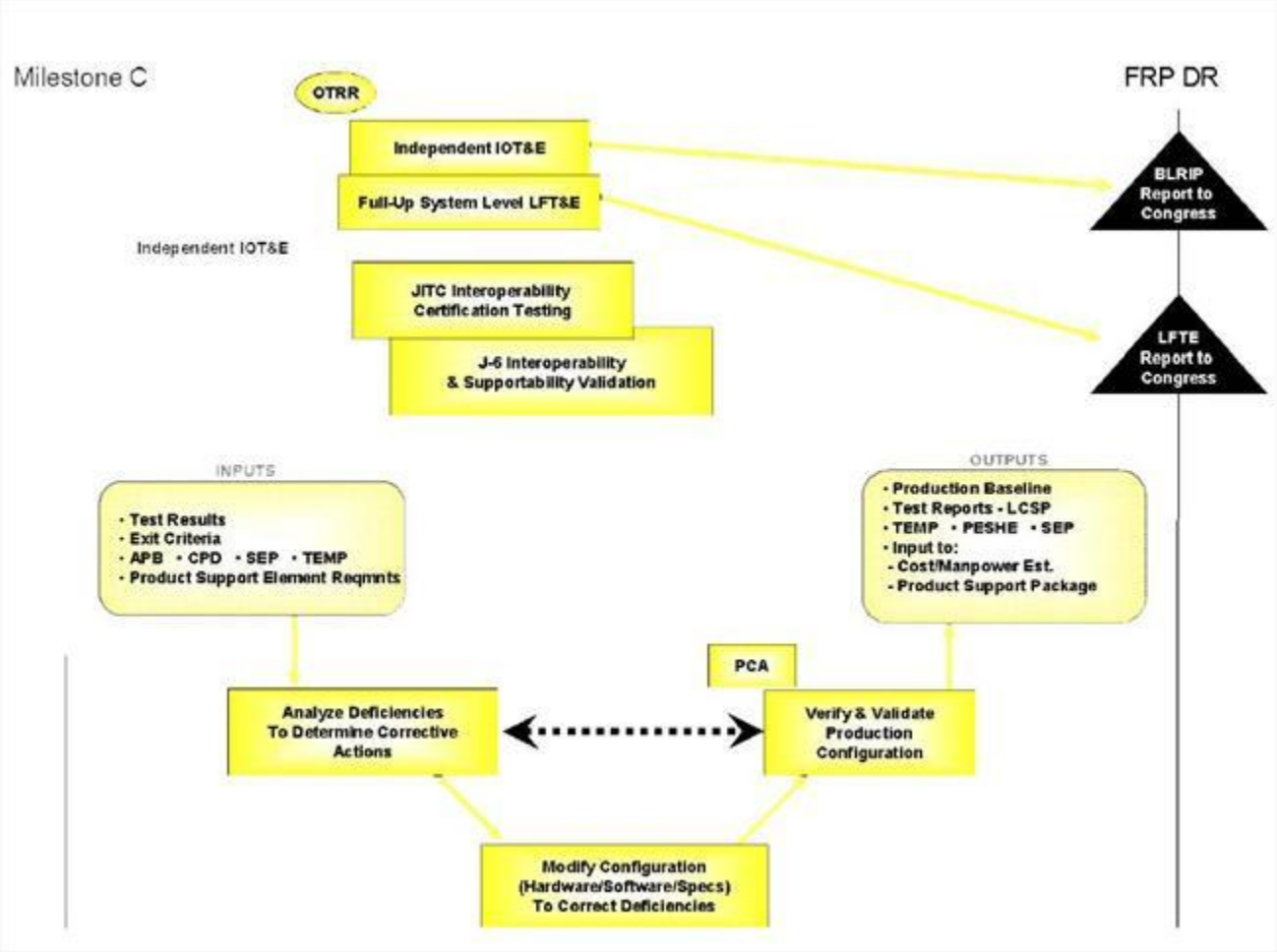


Figure 4.3.4.3.F1. Systems Engineering Activities During Production and Deployment

4.3.4.3.1. Analyze Deficiencies to Determine Corrective Actions

Using the aggregation of all inputs available at this stage of the program (test evaluation results, maintenance reports, exit criteria from Engineering and Manufacturing Development, Capability Production Document, Systems Engineering Plan, Test and Evaluation Master Plan, and Life-cycle Sustainment Plan), known deficiencies are analyzed. A solution is proposed through the employment of systems engineering processes including ESOH risk analysis. A plan to build, modify, verify, test and evaluate the proposed solution is formulated and approved.

4.3.4.3.2. Modify Configuration (Hardware, Software, and Specifications) to Correct Deficiencies

The proposed solution to the deficiency is translated to the appropriate hardware/software or specification changes. Modifications are created, incorporated, and verified in accordance with

the approved plan. This product change may include retrofit, because the production process has begun. The impact on system cost, schedules, and performance should also be considered when addressing production incorporation.

4.3.4.3.3. Verify and Validate Production Configuration

The proposed solution to the system deficiency should be verified and validated before incorporation into the production configuration. Depending on the nature of the change, this process may require analysis, laboratory, or full operational system test and evaluation. Any approved changes should be incorporated into the product baseline as an updated configuration.

4.3.5. Operations and Support Phase

The objective of this phase is the execution of a support program that meets operational support performance requirements and sustains the system in the most cost-effective manner over its total life cycle. When the system reaches the end of its useful life, the department should dispose of it. These two work efforts, sustainment and disposal, make up the Operations and Support phase.

Effective employment of systems engineering, applied in accordance with a well-structured Systems Engineering Plan, and monitored with meaningful technical reviews, will reduce program risk and identify potential management issues in a timely manner.

4.3.5.1. Purpose of Systems Engineering in Operations and Support

During the sustainment effort of the Operations and Support phase, systems engineering processes support in-service reviews including identifying root causes and resolutions for safety and critical readiness degrading issues. This effort includes participating in trade studies and decision making relative to the best resolution (e.g., changes to the product support package, process improvements, modifications, upgrades, and future increments of the system), considering the operational needs and the remaining expected service life. Interoperability or technology improvements, parts or manufacturing obsolescence, aging aircraft (or system) issues, premature failures, changes in fuel or lubricants, Joint or service commonality, etc. may all indicate the need for a system upgrade(s) or process improvements.

The last activity associated with the Operations and Support acquisition phase is disposal. Early systems engineering processes should include and inject disposal requirements and considerations into the design processes that ultimately facilitate disposal. System disposal is not typically a systems engineering activity.

4.3.5.2. Inputs to the Systems Engineering Processes in Operations and Support

- Service use data,
- Mishap data,
- User feedback,
- Failure reports,
- Discrepancy reports,
- Programmatic Environment, Safety, and Occupational Health Evaluation,
- Life-cycle Sustainment Plan,
- System Safety Analyses to include ESOH risk analysis (section 4.4.7.5), updating hazard analyses, and maintaining the hazard tracking system, and
- Systems Engineering Plan.

4.3.5.3. Key Systems Engineering Activities During Operations and Support

4.3.5.3. Key Systems Engineering Activities During Operations and Support

Figure 4.3.5.3.F1 illustrates the steps during the Operations and Support phase. Note: Given the iterative and recursive nature of systems engineering, the sequence of activities (displayed in the highlighted rectangles) is in their order of completion, vice the order of commencement. The activities can be started in any order and often run in parallel, but they should be completed in the order shown. Further detail on each step is contained in sections 4.3.5.3.1 through 4.3.5.3.7. Systems engineering should continue during operation and support of the system, and be used to continuously assess fielded system technical health against documented performance requirements and effectiveness, suitability, and risk measures. In-service systems engineering provides the program manager with an integrated technical assessment of system trends and sustainment alternatives, which is then used to oversee development and implementation of the selected alternative.

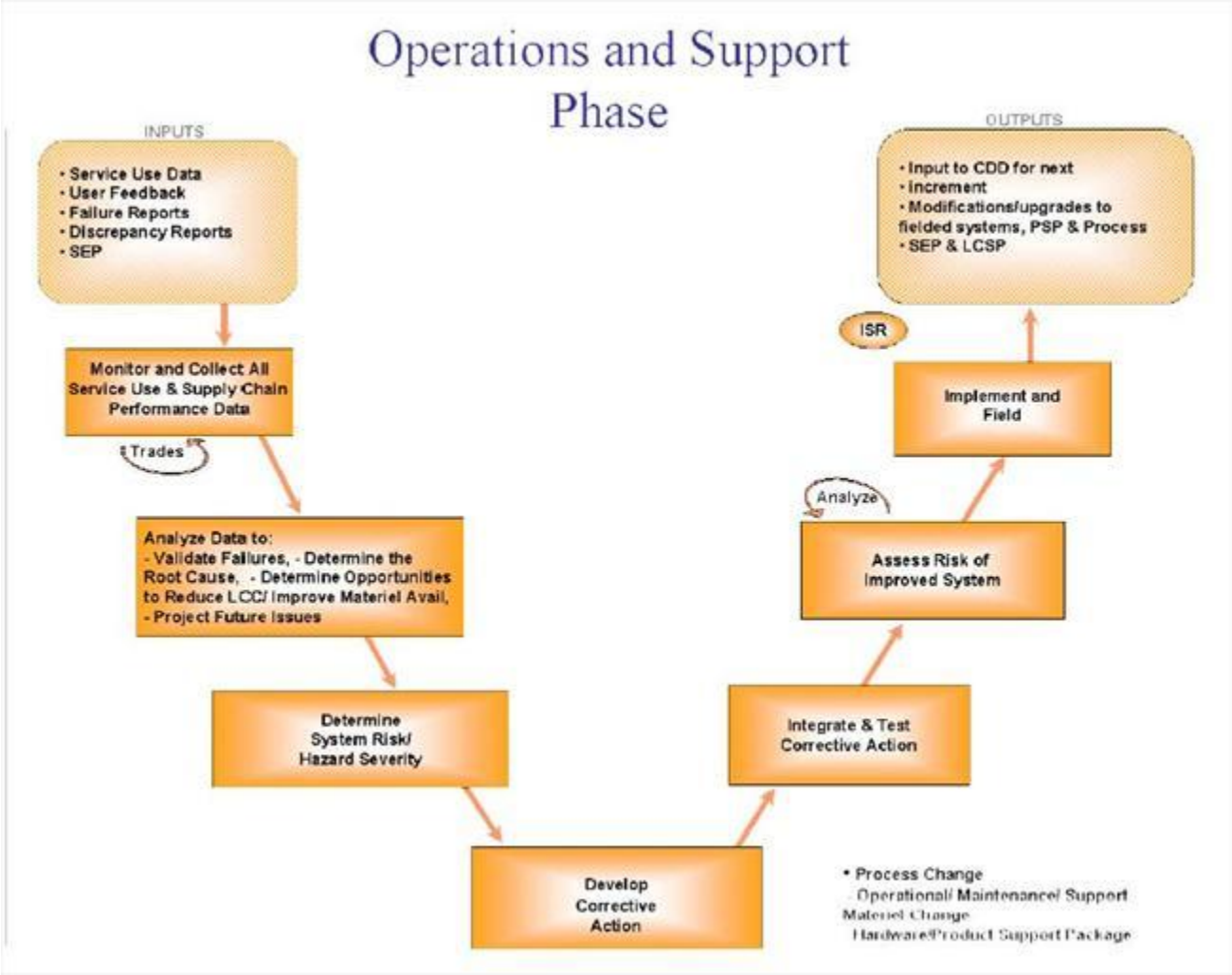


Figure 4.3.5.3.F1. Systems Engineering Activities During Operations and Support

4.3.5.3.1. Monitor and Collect All Service Use Data

The aggregation of all data inputs available at this stage of the program (service use data, maintenance discrepancy reports, user feedback, system/component failure reports, mishap data, and the Systems Engineering Plan provides the life-cycle basis for many operations and support decisions that will be made throughout the operational life of the system. Historically, many fielded systems remain in service much longer than originally planned. The type of data retrieved may change as the operational understanding of the system matures.

4.3.5.3.2. Analyze Data to Determine Root Cause of Problem

As problems arise in the fielded system, the systems engineering processes determine the cause of the problem and may lead to a solution. The retrieved data is a key to this determination, and should be thoroughly analyzed for causes and potential solutions. These analyses may ascertain whether deficiencies exist in the system as designed and built, or whether the system has been operated differently, or in a different environment, than that for which it was designed.

4.3.5.3.3. Determine the System Risk/Hazard Probability and Severity

Risk assessment techniques and principles, the methodology in MIL-STD-882D, "DoD Standard Practice for System Safety", as well as systems engineering processes determine the hardware and software safety hazards and identify the risks associated with identified hazards based on the probability and severity of the hazard.

4.3.5.3.4. Develop Corrective Action

Corrective actions (mitigation measures) may include process, hardware, software, support, materiel, or maintenance changes. The systems engineering process is used to develop appropriate corrective actions.

4.3.5.3.5. Integrate and Test Corrective Action

Integrate the proposed corrective actions (mitigation measures) and test to verify the corrective action is effective and the system/subsystem is suitable for fielding.

4.3.5.3.6. Assess Risk of Improved System

Once the effectiveness of the proposed corrective action is demonstrated, long-range system ramifications should be addressed. The appropriate systems engineering process is a risk assessment, which involves in-depth (regression, durability, structural, interoperability, support, etc.) system analyses. Additionally, the support, training, documentation, configuration, and maintenance aspects of the improvements should be considered. All of these elements have an impact on system life-cycle costs, which should be calculated to identify the required funding.

4.3.5.3.7. Implement and Field

Once authorized, the system corrective action/improvement can be implemented and fielded, along with adequate supplies, support, training, and maintenance procedures. Change documentation and configuration management should be maintained throughout this activity. This information can be used during periodic in-service reviews (ISRs) to assess in-service health, operational system risk, system readiness, costs, support trends, aging equipment and out-of-production issues.

4.3.5.4. Technical Review During Operations and Support: In-Service Review (ISR)

The ISR is a multi-disciplined product and process assessment to ensure that the system under review is operationally employed with well-understood and managed risk. This review is intended to characterize the in-service health of the deployed system. It provides an assessment of risk, readiness, technical status, and trends in a measurable form. These assessments substantiate in-service support budget priorities. The consistent application of sound programmatic, systems engineering, and logistics management plans, processes, and sub-tier in-service stakeholder reviews will help achieve the ISR objectives. Example support groups include the System Safety Working Group and the Integrated Logistics Management Team. A good supporting method is the effective use of available government and commercial data sources. In-service safety and readiness issues are grouped by priority to form an integrated picture of in-service health, operational system risk, system readiness, and future in-service support requirements.

The ISR should provide the following:

1. An overall System Hazard Risk Assessment (see section 4.4.7.5),
2. An operational readiness assessment in terms of system problems (hardware, software, and production discrepancies), and
3. Status of current system problem (discrepancy) report inflow, resolution rate, trends, and updated metrics. The metrics may be used to prioritize budget requirements.

Successful completion of this review should provide the program manager and other stakeholders with the integrated information they need to establish priorities and to develop execution and out year budget requirements.

Typical success outcomes include the following:

1. System problems have been categorized to support the operating and support requirements determination process.
2. Required budgets (in terms of work years) have been established to address all system problems in all priority categories.
3. Current levels of System Operational Risk and System Readiness have been quantified and related to current operations and systems and procurement budgets.
4. Future levels of System Operational Risk and System Readiness have been quantified and related to future year operations and systems and procurement budgets.

The ISR risk assessment checklist is designed as a technical review preparation tool, and should be used as the primary guide for assessing risk during the review. This checklist is available on the Systems Engineering Community of Practice.

4.3.5.5. Outputs of the Systems Engineering Processes in Operations and Support

- Input to Capability Development Document for next increment,
- Modifications and upgrades to fielded systems,
- System Safety Analyses to include ESOH risk analysis (section 4.4.7.5), sustaining hazard analyses for the fielded system, and input to the next increment,
- Data for next In-Service Review,
- Programmatic Environment, Safety, and Occupational Health Evaluation,
- Periodic updates to maintenance procedures through Reliability Centered Maintenance Analysis,
- National Environmental Policy Act (NEPA) Compliance Schedule (as required), and
- Systems Engineering Plan.

4.3.6. Evolutionary Acquisition Programs

Evolutionary acquisition strategies integrate advanced, mature technologies into producible systems that can be deployed to the user as quickly as possible. An evolutionary acquisition strategy matches available technology and resources to approved, time-phased, incremental delivery of capability needs. Systems engineering processes provide the disciplined, integrated development and production environment that supplies increasing capability to a materiel solution. In incremental development, capability is developed and fielded in increments with each successive increment building upon earlier increments to achieve an overall capability. These approaches to evolutionary acquisition are particularly effective in quickly fielding an initial capability or increment of functionality while allowing continued efforts to incrementally attain the final, full, end-state capability. Robust systems engineering processes ensure that systems are designed to easily and affordably accommodate additive capabilities in subsequent increments (e.g., modular, open systems design). The incremental development relies heavily on prototyping, both physical and functional, to get stakeholder feedback and reduce risk.

Evolutionary acquisition has increased the importance of traceability in program management. If a defense system has multiple increments, systems engineering can trace the evolution of the system. It can provide discipline to and documentation of the repeated trade-off analyses and decisions associated with the program. Because of the nature of evolutionary acquisition, design, development, deployment, and sustainment can each be occurring simultaneously for different system increments.

Programs with an evolutionary acquisition strategy undergo additional reviews (e.g., a Milestone B for each increment). The systems engineering activities and reviews are repeated as appropriate to ensure the same level of program insight is achieved within evolutionary acquisition programs.

4.3.1. Materiel Solution Analysis Phase

Program acquisition, beginning with Materiel Solution Analysis, presents the first substantial opportunity to influence systems design by balancing technology opportunities, schedule constraints, funding availability, and system performance parameters (including operational and sustainment requirements). Desired user capabilities, to be expressed in terms of key performance parameters and other quantifiable parameters, should be defined in terms of:

- System performance requirements (e.g., speed, lethality) to meet mission requirements, affordably, and
- The full range of sustainment requirements (materiel reliability, Materiel availability, mean down time, maintainability, logistics footprint, supportability criteria, etc.) needed to meet system sustainability over the long term.

Early and effective employment of systems engineering, applied in accordance with a well-structured Systems Engineering Plan , and monitored with meaningful technical reviews, will reduce program risk and identify potential management issues in a timely manner.

The Materiel Solution Analysis phase refines the initial concept and generates a Technology Development Strategy. Entrance into this phase requires a successful Materiel Development Decision and an approved Initial Capabilities Document. The Acquisition Decision Memorandum documents Milestone Decision Authority approval of the Analysis of Alternatives (AoA) plan and establishes a date for the Milestone A review. The Initial Capabilities Document and AoA plan guide the activities in the Materiel Solution Analysis phase.

4.3.1.1. Purpose of Systems Engineering in Materiel Solution Analysis

The Joint Capabilities Integration and Development System analysis process provides a structured methodology to identify capability gaps and needs, and suggest various approaches to provide needed capabilities within a specified functional or operational area. These analyses should incorporate innovative practices, including best commercial practices, collaborative environments, modeling and simulation, and electronic business solutions.

After the process identifies a materiel need, and an affirmative Materiel Development Decision initiates Materiel Solution Analysis, the Analysis of Alternatives (AoA) uses systems engineering processes to examine the materiel alternatives and identify a proposed solution. Systems engineering processes can provide a technical evaluation of the operational viability and relative costs of the alternative system concepts that may provide a materiel solution to a needed mission capability. The analysis should assess the advantages and disadvantages of the alternatives under consideration, including the design considerations, and include sensitivity analyses to possible changes in key assumptions or variables. Additionally, current policy requires the formulation of pending and future programs with strategies and funding that provide for two or more competing teams producing prototypes through (prior to) Milestone B.

During Materiel Solution Analysis, systems engineering processes should also support development of the Technology Development Strategy for the approved materiel solution.

4.3.1.2. Inputs to the Systems Engineering Processes in Materiel Solution Analysis

The following information sources provide important inputs to the systems engineering processes supporting materiel solution analysis:

- Initial Capabilities Document,
- Analysis of Alternatives Plan,
- Exit Criteria for the Materiel Solution Analysis Phase, and
- Alternative Maintenance and Sustainment Concept of Operations.

4.3.1.3. Key Systems Engineering Activities During Materiel Solution Analysis

4.3.1.3. Key Systems Engineering Activities During Materiel Solution Analysis

Figure 4.3.1.3.F1 identifies the systems engineering-related steps during the Materiel Solution Analysis phase. All decomposition activities listed below should be done concurrently for hardware and software. Note: Given the iterative and recursive nature of systems engineering, the sequence of activities (displayed in the highlighted rectangles) is in their order of completion,

vice the order of commencement. The activities can be started in any order, and often run in parallel, but should be completed in the order shown. Paragraphs below contain additional detail on each step.

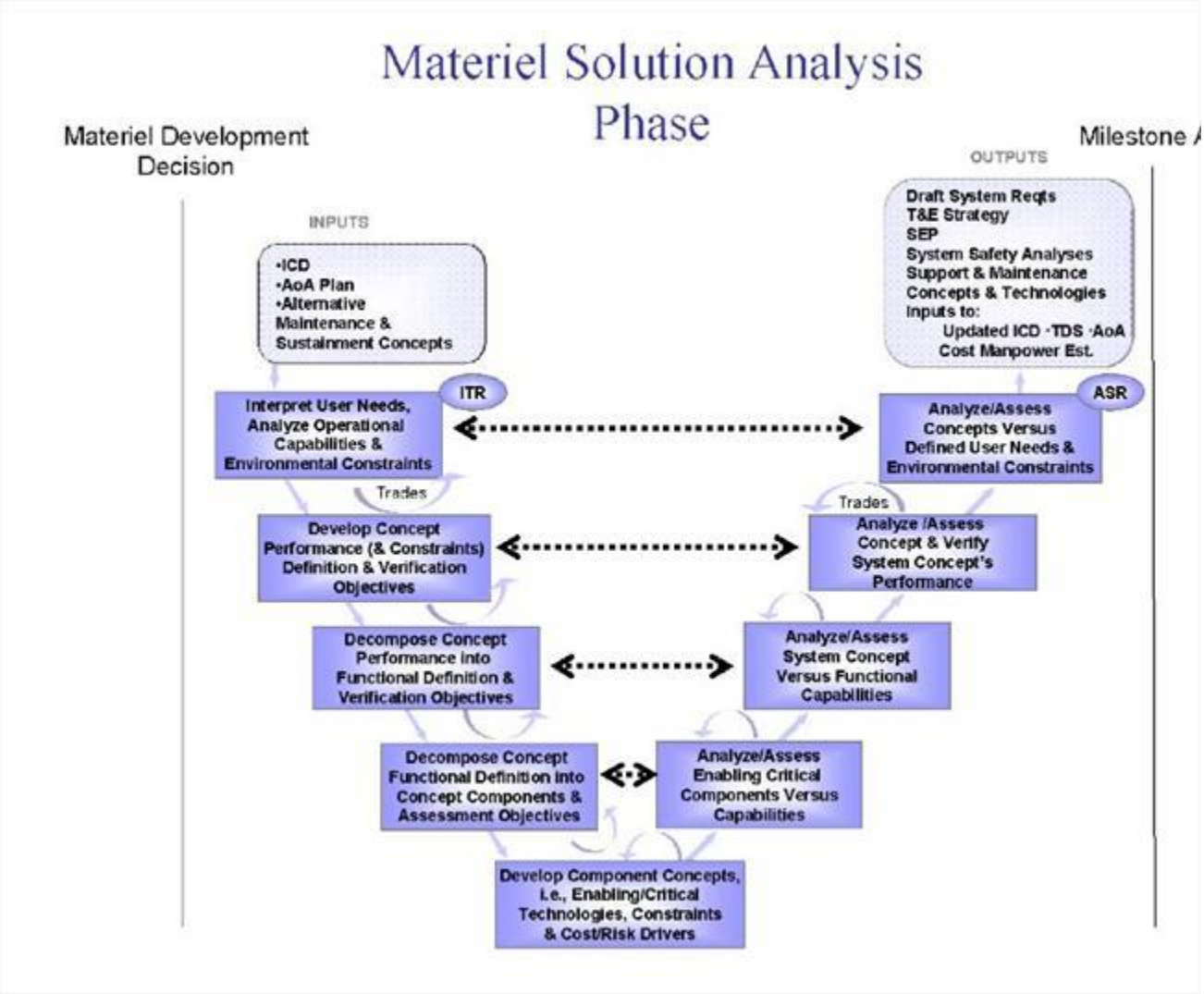


Figure 4.3.1.3.F1. Systems engineering-related steps during Materiel Solution Analysis

4.3.1.3.1. Interpret User Needs; Analyze Operational Capabilities and Environmental Constraints

This step includes the aggregation of all inputs available at this stage of the program (Initial Capabilities Document, Analysis of Alternatives Plan, exit criteria for the phase, concept alternatives for overall tactical system, as well as associated support system, training system, and

interoperable systems). Further analysis and definition is typically required to ascertain all of the related constraints to be applied to the effort. They include the following:

- Environmental: systems threats, usage environment, support environment, doctrine, operational concepts, (including installation/range Environmental, Safety and Occupational Health asset requirements),
- Resource: industrial base, notional available development, operation, and support budgets, initial operational capability and full operational capability dates,
- Technology: applicable technology base to be used for concept maturation, and
- Statutory and regulatory: applicable titles of the United states Code and public laws, the Federal Acquisition Regulation, the DoD 5000-series, etc.

Key to this initial step of Materiel Solution Analysis is to ensure that all drivers of the materiel solutions are completely captured and managed as an integrated whole, and all of the drivers can be met by each of the concept alternatives under consideration. This defines the expectations of the overall system concept, and defines the trade space and risk associated with each of the constraints listed above. Defining the trade space and risk enables comprehensive analysis of system alternatives, and allows a rational selection of a preferred system concept. The preferred system concept should strike the best balance in providing the needed capabilities within the constraints on the program.

4.3.1.3.2. Develop Concept Performance (and Constraints) Definition and Verification Objectives

This step includes the analysis and decomposition (from capability level to system level) of system performance and system design constraints traceable back to those capabilities and constraints defined in section 4.3.1.3.1 above. All capabilities and environmental constraints should be decomposed to the system performance level. They should be re-analyzed to determine the extent to which alternative concepts can meet all capability needs within program constraints (as needs and constraints become better understood as a result of decomposition). The trade space and risk should be analyzed and assessed for each alternative concept. For each alternative system concept, expected performance capabilities should be explicitly defined and related to the capability needs. To the extent concept performance can only be met through trade-offs (because of incompatibility of capabilities/constraints), changes may be required to the capability or constraints previously defined.

Verification planning should define the evaluation strategy to test and evaluate the ability of the materiel solution(s) matured system concept(s) to meet the capability needs and Joint Operational Concepts.

4.3.1.3.3. Decompose Concept Performance into Functional Definition and Verification Objectives

This step includes the further decomposition of concept system performance to the functional level. Consideration should be given to inclusion of functionality and functional flow definition across the full system concept (tactical system, support system, training system) and how this functionality relates to other interoperable systems (functional interfaces). Critical to this analysis is an understanding of the level of functionality achievable within program constraints and risk. Trade space and risk should be analyzed and assessed against desired functional performance. Trade-offs are made to stay within program constraints and may require changes to higher-level system or concept definitions.

System functional verification planning should enable test and evaluation of the matured system concept functionality.

4.3.1.3.4. Decompose Concept Functional Definition into Concept Components and Assessment Objectives

This step includes the allocation of concept functions into components of the concept that will execute the functionality. Critical to this analysis is an understanding of what functional performance is enabled by multiple systems, or system components, operating as a functional entity. Hardware elements, software elements, human elements, physical interfaces, functional interfaces, standards, existing, and to-be-developed elements, should all be considered and defined in the concept. As in previous steps, this level of decomposition and allocation may induce trades to stay within program constraints. These trades need to be reflected in higher-level functional, system, and capability definitions, which should be updated accordingly.

Concept component verification planning should enable testing and evaluation for validation of critical concept components.

4.3.1.3.5. Develop Component Concepts, Including Enabling/Critical Technologies, Constraints, and Cost/Risk Drivers

At this point, all of the basic concept design requirements should have been analyzed, defined, and reconciled with constraints. The system concept(s) components should have been synthesized and substantiated (e.g., through analyses, modeling and simulation, demonstrations, etc.) to allow verification of components against requirements, and integration of the components into an overall system for further verification and validation. Key to this step is the development of conceptual components to demonstrate the viability of the overall concept, indicate where additional technology maturation should occur, and validate that acceptable trade space between expected capabilities and program constraints exists to accommodate potential risk.

4.3.1.3.6. Analyze and Assess Enabling/Critical Components Versus Capabilities

Using the component verification plans developed as part of the functional allocation, the enabling and/or critical components of the concept should be evaluated. Evaluation results should be assessed against component requirements and the impact on the overall concept capabilities and constraints determined. Critical to this step is the understanding of test and evaluation results in demonstrating concept component functionality against desired capabilities, as well as determining required component technologies and levels of achievable performance. Capability trade-offs within the available trade space, or further component concept development within program and concept constraints, may be required.

4.3.1.3.7. Analyze and Assess System Concept Versus Functional Capabilities

Using the concept functional verification plans developed as part of the functional analysis and decomposition, overall system functionality should be evaluated. Concept components should be integrated and assessed from a functional standpoint relative to desired capabilities. Critical to this step is the understanding of how the enabling components work together as an integrated whole to provide functionality at the component and system levels, and how the achieved functionality relates to the overall desired capability. Also important is an understanding of the technology development required to achieve critical functions. Capability trade-offs within the available trade space, or further refinement of functionality within program and concept constraints may be required.

4.3.1.3.8. Analyze and Assess Concept and Verify System Concept's Performance

Using the verification objectives previously defined, the overall integrated concept should be evaluated against system performance objectives and constraints. Concept components are integrated from both physical and functional perspectives across the full concept domain (tactical, support, training, etc.). Critical to this step is an understanding of overall system concept capability versus need, level of achievable performance within the complete set of constraints, and the enabling technologies requiring further development. Trades at this level will include decisions as to acceptable technology risk versus desired performance.

4.3.1.3.9. Analyze and Assess Concepts Versus Defined User Needs and Specified Environmental Constraints

Based upon the results of the verification of components, functionality, and system performance, a determination of the preferred system concept should be made. Advantages and disadvantages of various approaches should be documented and included in the analysis of alternatives. Trade-offs of achievable performance should be complete and captured in a preliminary system specification. Enabling technologies requiring further development to achieve acceptable levels of risk should be defined and plans should be developed for technology development. The

preliminary system specification serves as the guiding technical requirement for this development effort.

4.3.1.4. Technical Reviews During Materiel Solution Analysis

4.3.1.4.1. Initial Technical Review (ITR)

The ITR is a multi-disciplined technical review to support a program's initial Program Objective Memorandum submission. This review ensures a program's technical baseline is sufficiently rigorous to support a valid cost estimate (with acceptable cost risk) and enable an independent assessment of that estimate by cost, technical, and program management subject matter experts (SMEs). The ITR assesses the capability needs and Materiel solution approach of a proposed program and verifies that the requisite research, development, test and evaluation, engineering, logistics, and programmatic bases for the program reflect the complete spectrum of technical challenges and risks. Additionally, the ITR ensures the historical and prospective drivers of system life-cycle cost have been quantified to the maximum extent and that the range of uncertainty in these parameters has been captured and reflected in the program cost estimates.

Per DoD Instruction 5000.02, Enclosure 7, paragraph 2, the program manager for Acquisition Category I and IA programs shall define program and system parameters in a Cost Analysis Requirements Description (CARD), as described in DoD 5000.4-M.

The basic CARD technical and programmatic guidance, tailored to suit the scope and complexity of the program, should be followed to ensure all pertinent design-related cost drivers are addressed. The success of the ITR also depends on independent SME review of each of the identified cost drivers. The SMEs should be drawn from the correct technical competencies that specialize in each of the areas addressed in a CARD-like document (i.e., basis of estimate), and the cost drivers detailed in the CARD-like document should be used properly in the development of the program cost estimate. Completion of the ITR should provide:

1. A complete CARD-like document detailing the operational concept, candidate materiel solutions, and, risks,
2. An assessment of the technical and cost risks of the proposed program, and
3. An independent assessment of the program's cost estimate.

Typical ITR success criteria include affirmative answers to the following exit questions:

1. Does the CARD-like document capture the key program cost drivers, development costs (all aspects of hardware, human integration, and software), production costs, operation and support costs?
2. Is the CARD-like document complete and thorough?
3. Are the underlying assumptions used in developing the CARD-like document technically and programmatically sound, executable, and complete?
4. Have the appropriate technical and programmatic competencies been involved in the CARD-like document development, and have the proper SMEs been involved in its review?
5. Are the risks known and manageable within the cost estimate?
6. Is the program, as captured in the CARD-like document, executable?

The ITR risk assessment checklist is designed as a technical review preparation tool, and should be used as the primary guide for assessing risk during the review. This checklist is available on the Systems Engineering Community of Practice.

4.3.1.4.2. Alternative Systems Review (ASR)

The ASR is a multi-disciplined technical review to ensure the resulting set of requirements agrees with the customers' needs and expectations and the system under review can proceed into the Technology Development phase. The ASR should be completed prior to, and provide information for Milestone A. Generally, this review assesses the preliminary materiel solutions that have been evaluated during the Materiel Solution Analysis phase, and ensures that the one or more proposed materiel solution(s) have the best potential to be cost effective, affordable, operationally effective and suitable, and can be developed to provide a timely solution to a need at an acceptable level of risk. Of critical importance to this review is the understanding of available system concepts to meet the capabilities described in the Initial Capabilities Document (ICD) and to meet the affordability, operational effectiveness, technology risk, and suitability goals inherent in each alternative concept.

Acquisition policy requires prototyping in the Technology Development phase. Therefore, the ASR should identify key system elements that two or more competing teams will prototype prior to Milestone B. The intent is to reduce technical risk, validate designs, validate cost estimates, evaluate manufacturing processes, and refine requirements. The ASR identifies the most promising path forward; however; there is still the understanding that both the requirements and the system may evolve until Milestone B.

By reviewing alternative materiel solutions, the ASR helps ensure that sufficient effort has been given to conducting trade studies that consider and incorporate alternative system designs that may more effectively and efficiently meet the defined capabilities. A successful review is predicated on the Integrated Product Team's determination that the operational capabilities, proposed solution(s), available technologies, and program resources (funding, schedule, staffing, infrastructure, and processes) form a satisfactory basis for proceeding into the Technology

Development phase. The program manager should tailor the review to the technical scope and risk of the system, and address the ASR in the Systems Engineering Plan.

Completion of the ASR should provide the following:

1. An agreement on the proposed materiel solution(s) (including the corresponding product support concept) to take forward into the milestone decision and subsequent Technology Development phase.
2. Hardware and software architectural constraints/drivers to address all key performance parameters (KPPs) (e.g., materiel availability, net-centric and net ready KPP requirements).
3. An assessment of the full system software concept to include conceptual definition of the complete deliverable/non-deliverable software, scope, and risk (e.g., operational software elements, software engineering environment, test software, maintenance software, simulation/stimulation software, training software, in-service support software, etc.).
4. A comprehensive rationale for the proposed materiel solution(s), based upon the Analysis of Alternatives that evaluated relative cost, schedule, performance (hardware, human, software), and technology risks.
5. A comprehensive assessment of the relative risks associated with including commercial off-the-shelf items in the program, with emphasis on host platform environmental design, diagnostic information integration, and maintenance concept compatibility.
6. A comprehensive risk assessment for the Technology Development phase.
7. Results of trade studies/technical demonstrations for concept risk reduction.
8. Joint requirements for the purposes of commonality, compatibility, interoperability, and integration.
9. Refined thresholds and objectives initially stated as broad measures of effectiveness and suitability (e.g., KPPs/key system attributes).
10. Completed, comprehensive planning for the Technology Development phase (hardware, software and human systems), including critical components to be developed, prototyped, and demonstrated, their cost, and critical path drivers. This planning could include and integrated Master Plan and Integrated Master Schedule.
11. Initial planning for the Engineering and Manufacturing Development phase.
12. A draft system requirements document if one does not already exist. (This is a high-level engineering document that represents the customer/user capability needs as system requirements.) This systems requirement document should include a system level description of all software elements required by the preferred system concept.

The ASR is important because it is a comprehensive attempt to ensure the system requirements are aligned with the customer's needs. The ASR attempts to minimize the number of requirements that may need to be changed in later phases. Changing requirements later in the program will usually entail cost increases and scheduling slips.

1. Can the proposed materiel solution(s) satisfy the ICD, which may have been adjusted (in accordance with Joint Capabilities Integration and Development System procedures) for Cost As an Independent Variable?
2. Is the proposed materiel solution(s) sufficiently detailed and understood to enable entry into Technology Development with low technical risk?
3. Are the system software scope and complexity sufficiently understood and addressed in the planning for the Technology Development phase to enable an acceptable/manageable level of software technical risk?
4. Have the preliminary manufacturing processes and risks been identified for prototypes?
5. Are the risks for competitive prototyping and initial development (through to the allocated baseline) known and manageable?
6. Is the Technology Development work effort properly staffed?
7. Is the Technology Development work effort executable within the existing budget and schedule?
8. Has a preliminary system specification, consistent with technology maturity and the proposed program cost and schedule, been captured in the system technical baseline?
9. Have required investments for technology development, to mature design and manufacturing related technologies, been identified and funded?
10. Have initial producibility assessments of design concepts been completed?
11. Is the program schedule for the Technology Development Phase executable (technical/cost risks)?
12. Are the hazards sufficiently understood and addressed to achieve an acceptable/manageable level of ESOH risk in the Technology Development phase?

The ASR risk assessment checklist is designed as a technical review preparation tool, and should be used as the primary guide for assessing risk during the review. This checklist is available on the Systems Engineering Community of Practice.

4.3.1.5. Summary of Outputs of the Systems Engineering Processes in Materiel Solution Analysis

- Preliminary System Specification,
- Test and Evaluation Strategy,
- System Safety Analyses (ensure a Preliminary Hazard List is completed for each system concept),
- Systems Engineering Plan (to include competitive prototype planning),
- Support and Maintenance Concepts and Technologies,
- Inputs to draft Capability Development Document,
- Inputs to Technology Development Strategy, to include competitive prototype planning,
- Inputs to Analysis of Alternatives (AoA), and
- Inputs to Cost and Manpower Estimate.

4.4. Systems Engineering Design Considerations

Subordinate sections to 4.4 cover the following topics:

4.4. Systems Engineering Design Considerations

The program manager faces a myriad of considerations and management tools to translate the user's desired capabilities (regardless of the phase in the acquisition cycle) into a structured system of interrelated design specifications. This is a complex task. It is an iterative task, performed within the framework of Systems Engineering to achieve the 'best value' for the user.

The 'best value' solution is not easy to define. Many requirements and design considerations cannot fully coexist in a single design; hence, the need for rigorous systems engineering processes with trade-offs to develop a balance solution. The systems engineering processes detailed in Section 4.2 and applied in each acquisition phase as detailed in Section 4.3 will enable the program manager to manage expectations of the user across the spectrum of requirements and design. The systems engineering management tools discussed in Section 4.5 give the program manager the methodology to examine the specific characteristics of the program against a myriad of often-conflicting design considerations. This Section discusses a number of these considerations and how they contribute to program performance, cost effectiveness, reduced development cycle time, and improved supportability. The design considerations are listed alphabetically, not in an order of importance. The order of importance will vary with each program and result in a different, optimal solution depending on the capabilities required of the program.

Some design considerations apply only to single systems while others apply to both individual as well as the system of systems. Additionally, some design considerations such as interoperability requirements and open interface standards needed to bind constituent systems in a system of systems are design requirements that do not allow trade space. Some design considerations will take the form of design constraints (e.g., weight, volume, power, cooling, etc.) and will need to be closely managed through a rigorous trade process. Some constraints may need to be managed as system-wide budgets and require close tracking as the design matures. The challenge for the program manager is to apply systems engineering to achieve balance across all of the considerations and constraints.

The program manager should be aware that some considerations are mandated by laws and regulations and others will be mandated by the user in the program's capability document. These mandates should be optimally balanced in the design process.

Figure 4.4.F1 provides a framework for how these design considerations fit into an affordable systems operational effectiveness framework.

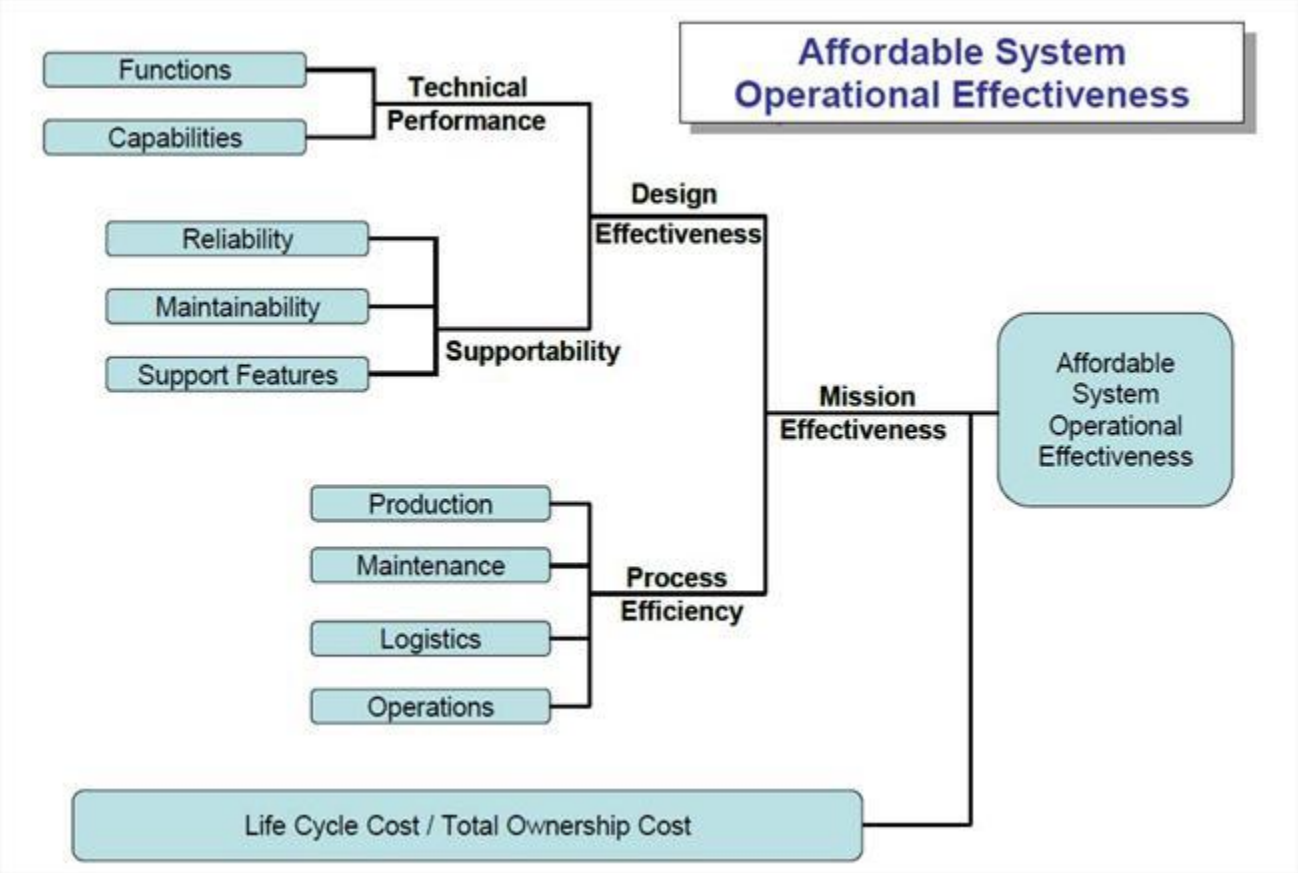


Figure 4.4.F1. Affordable System Operational Effectiveness Diagram

4.4.1. Accessibility

The program manager must ensure that electronic and information technology acquisitions comply with Section 508 of the Rehabilitation Act of 1973. Unless an exception at Federal Acquisition Regulation 39.204 applies, acquisitions of electronic and information technology supplies and services must meet the applicable accessibility standards at Title 36 Code of Federal Regulations Section 1194. To avoid unnecessary costs and delays, the program manager should consider what accessibility requirements, if any, are applicable to the program early and throughout the system life cycle.

4.4.2. Commercial Off-the-Shelf (COTS)

Use of COTS items offers significant opportunities for reduced development time, faster insertion of new technology, and lower life-cycle costs, owing to a more robust industrial base. Maximum use of commercially mature technology provides the greatest opportunity to meet program cost, schedule, and performance requirements and is consistent with an evolutionary acquisition strategy. However, regardless of the extent to which a system is made up of

commercial items, the program manager still engineers, develops, integrates, tests, evaluates, delivers, sustains, and manages the overall system. The program manager should pay particular attention to the intended product use environment and understand the extent to which this environment differs from (or is similar to) the commercial use environment. Subtle differences in product use can significantly impact system effectiveness, safety, reliability, and durability.

The marketplace drives COTS product definition, application, and evolution. COTS products presume a flexible architecture (in most cases an open architecture) and most often depend on product releases that are designed to be used "as is" to meet general business needs, not a specific organization's needs. Consequently, if a program purchases a "modified COTS product" (which, by definition, is not a COTS product) or modifies a COTS product on its own, then the program may lose the ability to use the vendor's subsequent product upgrades or to find a suitable replacement for the product from other commercial sources. Moreover, COTS products require continuous monitoring of the commercial marketplace through market research activities and continuing alignment of business and technical processes, and impose additional cost, schedule, and performance risks that the acquisition community should pay attention to and plan for.

When acquiring COTS software products or other commercial items, the program manager still implements systems engineering processes. In this context, integration encompasses the amalgamation of multiple COTS components into one deployable system or the assimilation of a single COTS product (such as an enterprise resource planning system). In either case, the program manager should ensure that the system co-evolves with essential changes to doctrine (for combat systems) or reengineered business processes (for combat support and information technology systems) and apply commercial item best practices in the following areas:

- Adapting to commercial business practices,
- COTS evaluation,
- Life-cycle planning(including sustainment, obsolescence and disposal),
- Relationship with vendors,
- Test and evaluation of COTS items, and
- Protection of intellectual property rights.

Adapting to Commercial Business Practices. When purchasing a commercial item, the program manager should adopt commercial business practice(s). The extent to which the DoD business practices match the business practices supported by commercial items determines the likelihood that the items will meet DoD needs, yet still realize the intended cost savings. It is likely, however, that a user requirements gap will exist, and the gap may be large. Negotiation, flexibility, and communication on the part of the stakeholders, the commercial vendors, and the program manager are required. Moreover, when purchasing a commercial item, the program manager should ensure that the system as well as the commercial item component utilizes open standards in their external interfaces to facilitate integration, permit insertion of new technology embedded in COTS products, and enable future replacement with similar items from competitive sources.

COTS Evaluation. The program manager should plan for and implement evaluations to assist in fully identifying commercial capabilities, to choose between alternate architectures and designs, to determine whether new releases continue to meet requirements, to conform to open architecture standards, and to ensure that the commercial items function as expected when linked to other system components without creating unacceptable safety hazards. In addition, evaluation provides the critical source of information about the trade studies that should be made between the capabilities of the system to be fielded and the system architecture and design that makes best use of commercial capabilities. Evaluating commercial items requires a focus on mission accomplishment and matching the commercial item to system requirements.

For COTS software, program managers are encouraged to use code-scanning tools, within the scope and limitations of the licensing agreements, to ensure both COTS and government off-the-shelf software do not pose any information assurance or security risks. Section 7.10 of this guidebook discusses the considerations for COTS software solutions.

For COTS devices that use the electromagnetic spectrum (e.g., spectrum-dependent), program managers should be aware that COTS devices that are authorized to operate within the United States and its possessions are not automatically authorized to operate in foreign countries outside the United States and its possessions. Examples of such COTS devices include radio frequency identification systems, wireless local-area-networks, baby monitors, and garage door openers. Chapter 7 lists the policy documents relating to electromagnetic spectrum management and describes the procedures for obtaining spectrum supportability.

Life-cycle Planning. The program manager should establish a rigorous change management process for life-cycle support. Systems that integrate multiple commercial items require extensive engineering to facilitate the insertion of planned new commercial technology. This is not a "one time" activity because unanticipated changes (such as a commercial vendor's decision to cease producing a particular product or component) may drive reconsideration of engineering decisions throughout the life of the program. Failure to address changes in commercial items and the marketplace will potentially result in a system that cannot be maintained as vendors drop support for obsolete commercial items.

Relationship with Vendors. The program manager needs to remain aware of and influence product enhancements with key commercial item vendors to the extent practical. As vendors are different from contractors and subcontractors, different practices and relationships are needed. Vendors react to the marketplace, not the unique needs of DoD programs. To successfully work with vendors, the program manager may need to adopt practices (e.g., use of open architecture) and expectations that are similar to other buyers in the marketplace. Traditional DoD acquisition and business models are not sufficient for programs acquiring commercial items, as they do not take into account the marketplace factors that motivate vendors.

Test & Evaluation of COTS Items. The program manager should develop an appropriate test and evaluation strategy for commercial items to include evaluating potential commercial items in a system test bed, when practical, focusing test beds on high-risk items, and testing commercial-

item upgrades for unanticipated side effects in areas such as security, safety, reliability, and performance. It is essential to integrate this test and evaluation strategy with life-cycle planning as described above.

Protection of Intellectual Property Rights. Intellectual Property (IP) consists of patents, copyrights, trademarks, and trade secrets. Programs need to be aware of pertinent intellectual property right issues associated with commercial items acquisitions (by consulting with their program attorneys), especially with the acquisition of commercial software products. When acquiring IP license rights, the acquisition community should consider the following core principles as described in a DoD guide entitled: Intellectual Property: Navigating through Commercial Waters.

- Integrate IP considerations fully into acquisition strategies for advanced technologies to protect core DoD interests,
- Respect and protect privately developed IP because it is a valuable form of intangible property that is critical to the financial strength of a business,
- Resolve issues before award by clearly identifying and distinguishing the IP deliverables from the license rights in those deliverables,
- Negotiate specialized IP provisions whenever the customary deliverables or standard license rights do not adequately balance the interests of the contractor and the government, and
- Seek flexible and creative solutions to IP issues, focusing on acquiring only those deliverables and license rights necessary to accomplish the acquisition strategy.

4.4.3. Corrosion Prevention and Control

DoD Instruction 5000.02, Enclosure 12, paragraph 7, directs that:

As part of a long-term DoD corrosion prevention and control strategy that supports reduction of total cost of system ownership, each ACAT I program shall document its strategy in a Corrosion Prevention Control Plan. The Plan shall be required at Milestones B and C. Corrosion considerations shall be objectively evaluated throughout program design and development activities, with trade-offs made through an open and transparent assessment of alternatives.

The program manager should consider and implement corrosion prevention and mitigation planning to minimize the impact of corrosion and material deterioration throughout the system life cycle (see the Corrosion Prevention and Control Planning Guidebook). Corrosion prevention and mitigation methods include, but are not limited to, the use of effective design practices, material selection, protective finishes, production processes, packaging, storage environments, protection during shipment, and maintenance procedures. The program manager establishes and maintains a corrosion prevention and mitigation reporting system for data collection and feedback and uses it to address corrosion prevention and mitigation logistic considerations and readiness issues. Corrosion prevention and mitigation considerations are integral to all trade-off decisions as required in DoD Directive 5000.01 E1.1.17:

Performance-Based Logistics. PMs shall develop and implement performance-based logistics strategies that optimize total system availability while minimizing cost and logistics footprint. Trade-off decisions involving cost, useful service, and effectiveness shall consider corrosion prevention and mitigation. Sustainment strategies shall include the best use of public and private sector capabilities through government/industry partnering initiatives, in accordance with statutory requirements.

4.4.4. Critical Safety Items (CSIs)

CSIs are parts whose failure could cause loss of life, permanent disability or major injury, loss of a system, or significant equipment damage. Special attention has been placed on CSIs because of the potential catastrophic or critical consequences of failure and because DoD has experienced problems in the past, particularly when CSIs were purchased from suppliers with limited knowledge of the items' design intent, application, failure modes, failure affects, or failure implications. Public law 108-136, sec 802 was enacted to address aviation CSIs, and Public Law 109-364, sec 130 was enacted to address ship CSIs. Portions of these laws were codified in 10 U.S.C. 2319.

Department of Defense and Service policies also have been issued to address CSIs. DoD 4140.1-R, "DoD Supply Chain Materiel Management Regulation," establishes top-level procedures for the management of aviation CSIs. Additionally, a joint Military Service/Defense Agency instruction on "Management of Aviation Critical Safety Items" was issued on 25 January 2006. This instruction (SECNAVINST 4140.2, AFI 20-106, DA Pam 95-9, DLAI 3200.4, and DCMA INST CSI (AV)) specifically addresses requirements for identifying, acquiring, ensuring quality, managing, and disposing of aviation CSIs. The Joint Aeronautical Logistics Commanders also issued the Aviation Critical Safety Items (CSIs) Handbook. This guidance establishes standard user-level operating practices for aviation CSIs across the Services, the Defense Logistics Agency, the Defense Contract Management Agency, and other federal agencies. Additional Service and agency-specific aviation CSI implementing policies and guidance have been issued. Similar policies, procedures, and guidance are being developed and/or revised to address ship CSIs as defined by public law.

The public laws address three specific issues. First, they establish that the Design Control Activity (DCA) is responsible for processes concerning the management and identification of CSIs used in procurement, modification, repair, and overhaul of aviation and ship systems. The DCA is defined in law as the systems command of a military Service responsible for the airworthiness or seaworthiness certification of the system in which a CSI is used. Second, the laws require that DoD only enter into contracts involving CSIs with sources approved by the DCA. Finally, the laws require that CSI deliveries and services performed meet all technical and quality requirements established by the DCA.

The Defense Federal Acquisition Regulation Supplement (DFARS) was amended to implement the contractual aspects of the public law regarding aviation CSIs. Comparable DFARS amendments are in the works to address ship CSIs. DFARS 209.270 states that the DCA will:

- Identify items that meet aviation CSI criteria,
- Approve qualification requirements, and
- Qualify suppliers.

This section states that the contracting activity will contract for aviation CSIs only with suppliers approved by the DCA. DFARS 246.407 was amended to state that only the DCA can authorize acceptance of nonconforming aviation CSIs; however, DCA authority can be delegated for minor nonconformance. DFARS 246.504 requires DCA concurrence before certificates of conformance are used to accept aviation CSIs. Because contractors may uncover problems with products after items are delivered, DFARS 246.371 and 252-246.7003 requires contractors to notify the procuring and contracting officers within 72 hours after discovering or obtaining credible information that a delivered CSI, or a subsystem or system, may have discrepancies that affect safety.

The intent of CSI laws, regulations, policies, and guidance is to mitigate hazards from the receipt of defective, suspect, improperly documented, unapproved, and fraudulent parts having catastrophic potential. CSI policies ensure that items of supply that are most critical to operational safety are rigorously managed and controlled in terms of supplier capability; conformance to technical requirements; controls on changes or deviations; and inspection, installation, maintenance, and repair requirements, etc.

To ensure adequate management of CSIs throughout a system's Operations and Support phase, program managers should ensure CSIs are identified and documented in sufficient time to influence critical down-stream processes such as initial provisioning, supply support, and manufacturing planning. Prior to the Critical Design Review (CDR): the program office, with support from the DCA and prime/Original Equipment Manufacturer (OEM) contractors, should ensure that there is a clear understanding of CSI processes, terms, and criteria. Provisions should be made for prime/OEM contractors to deliver an initial list of recommended CSIs that are available for review at CDR. As the design, product baseline, production processes, and supportability analyses mature, the CSI list should continue to evolve. Throughout Low-Rate Initial Production (if applicable), conduct of the Physical Configuration Audit, and establishment of the final product baseline, the CSI list should be updated and reviewed to ensure it reflects the current situation. Before the Full-Rate Production Decision Review, a final CSI list should be documented and approved by the DCA.

4.4.5. Disposal and Demilitarization

The program manager should consider materiel demilitarization and disposal during systems engineering as part of the program manager's Total Life-cycle Systems Management responsibilities. The program manager should minimize the environmental and personnel risks associated with decontamination, decommissioning, demilitarization, and disposal of the system; all hazardous materials used on the system shall be identified, quantified, and mapped by location on the system. The program manager should coordinate with DoD component logistics and explosive safety activities and the Defense Logistics Agency, as appropriate, to identify and

apply applicable demilitarization requirements necessary to eliminate the functional or military capabilities of assets and to determine reutilization and hazardous-property disposal requirements for system equipment and by-products (see DoD 4140.1-R; and DoD 4160.21-M-1).

For a conventional ammunition program, the use of energetic materials implies unique challenges in the demilitarization phase of the life cycle and requires special considerations during development. "Demil" considerations and requirements should be included in the Systems Engineering process (i.e., "design for demil") and are guided by an understanding of the impact of design features on ultimate demil operations (DoD Instruction 5000.02, Enclosure 2, paragraph 8.c.(2)). Open burn and open detonation are not to be considered the primary methods of demilitarization or disposal. Rather, varieties of chemical and mechanical processes are used to accomplish demilitarization. The need to efficiently process the munition during demil should be considered during design and the cost to conduct these demil operations are included in total life cycle cost. Additionally, opportunities exist to recover value for the DoD through the recycling of materials or reuse of components, if the munitions design allows it to be done economically. Personnel safety should also be considered due to the required handling of munitions during demil. And end of life cycle environmental impacts are determined by material selection during design.

Conventional ammunition designs should provide for easy disassembly into component parts and allow easy removal of energetic materials, economical recovery of materials and components for recycle and reuse, efficient processing through demil equipment, safe handling, and minimal environmental impact. The type and weight of munition components, parts, and materials should be documented to provide transparency for future demil operations. The effectiveness of design for demil can be maximized while minimizing cost impact to the program by defining and incorporating demil considerations and requirements early and maintaining them as an inherent part of the design process. Additional resources and information can be obtained at the Product Manager for Demilitarization website.

4.4.6. Diminishing Manufacturing Sources and Material Shortages (DMSMS)

DMSMS is the loss, or impending loss, of manufacturers of items or suppliers of items or raw materials. The DoD loses a manufacturer when that manufacturer discontinues (or plans to discontinue) production of needed components or raw materials. This can be caused by many factors including new or evolving science, detection limits, toxicity values, and regulations related to chemicals and materials, resulting in significant impact on DoD's supply chain and industrial base. This situation may cause shortages that endanger the life-cycle support and capability of the weapon system or equipment. An effective approach to such a pervasive problem hinges on being proactive so that potential availability problems are resolved before they cause an impact in readiness or spending. SD-22, "Diminishing Manufacturing Sources and Material Shortages (DMSMS) Guidebook," provides more information on related design considerations.

While DMSMS can have a huge impact on total life-cycle cost, parts management is a strategy for mitigation or avoiding DMSMS problems. Systems Engineering Plans should include a robust section on parts management. Section 4.4.12 provides more detailed information on this topic.

4.4.7. Environment, Safety, and Occupational Health (ESOH)

4.4.7. Environment, Safety, and Occupational Health (ESOH)

ESOH planning and execution is integral to the systems engineering process for all developmental and sustaining activities. As part of the program's overall risk reduction, the program manager should eliminate ESOH hazards, where possible, and manage their associated risks where hazards cannot be eliminated (see section 6.3.5). DoD Instruction 5000.02, Enclosure 12, paragraph 6, requires program managers to manage ESOH risks for their system's life cycle using the methodologies described in MIL-STD-882D, "DoD Standard Practice for System Safety".

The PM shall integrate ESOH risk management into the overall systems engineering process for all developmental and sustaining engineering activities. As part of risk reduction, the PM shall eliminate ESOH hazards where possible, and manage ESOH risks where hazards cannot be eliminated. The PM shall use the methodology in MIL-STD-882D, "DoD Standard Practice for System Safety"...

Effective ESOH efforts encompass establishing ESOH responsibilities within the acquisition program's organizational structure; developing strategies to ensure compliance with ESOH regulatory requirements; identifying and managing hazardous materials, wastes, and pollutants for the life cycle of the system (including demilitarization and disposal); identifying and tracking the mitigation of ESOH hazards and associated risks; and formally accepting and communicating identified ESOH risks and their associated mitigations, including obtaining formal user representative concurrence on high and serious risks.

Additional detailed guidance, processes, and tools are available at the ESOH Special Interest Area on the Acquisition Community Connection web site, and at the DAU-hosted System Safety in Systems Engineering continuous learning module (click on CLE009).

4.4.7.1. Programmatic Environmental, Safety and Occupational Health (ESOH) Evaluation (PESHE)

As part of executing ESOH requirements, program managers must prepare a Programmatic ESOH Evaluation regardless of the program's acquisition category.

The program manager for all programs, regardless of ACAT level, shall prepare a PESHE which incorporates the MIL-STD-882D process and includes the following: identification of ESOH responsibilities; the strategy for integrating ESOH considerations into the systems engineering process; identification of ESOH risks and their status; a description of the method for tracking hazards throughout the life cycle of the system; identification of hazardous materials, wastes, and pollutants (discharges/emissions/noise) associated with the system and plans for their minimization and/or safe disposal; and a compliance schedule covering all system-related activities for the NEPA (42 U.S.C. 4321-4347, Reference (aa)) and EO 12114 (Reference (ab)). The Acquisition Strategy shall incorporate a summary of the PESHE, including the NEPA/EO 12114 compliance schedule.

A current PESHE document is required at Program Initiation for Ships, Milestone B, Milestone C, and the Full-Rate Production Decision Review. It is recommended that the PESHE be updated for the Critical Design Review. The PESHE document serves as a repository for top-level ESOH management information to include:

- Identification, assessment, mitigation, and acceptance of ESOH risks,
- On-going evaluation of mitigation effectiveness, and
- Compliance Schedule for National Environmental Policy Act (NEPA) (see section 4.4.7.2; Section 4321 et seq. of Title 42, United States Code, "National Environmental Policy Act;" and Executive Order (EO) 12114, "Environmental Effects Abroad of Major Federal Actions") documentation.

The PESHE document communicates to program managers and others the status of the ESOH effort and ESOH risk management for the system. The Acquisition Strategy must also include a summary of the PESHE and the NEPA/EO 12114 Compliance Schedule. When the Acquisition

Strategy is prepared before the PESHE, the Acquisition Strategy should define the overall approach for integrating ESOH into systems engineering, including roles and responsibilities for executing the strategy, and include an initial NEPA/EO 12114 Compliance Schedule. The PESHE should be consistent with the Acquisition Strategy's ESOH discussion. The Systems Engineering Plan (SEP) should also include a reference to the strategy for integrating ESOH into the systems engineering process as documented in the PESHE.

At Milestone B, the PESHE serves as an initial planning document. Thereafter, the PESHE documents the status of the program's ESOH efforts, including risk management. As the program matures, the PESHE provides further details on the status of ESOH efforts and risks. The program manager documents the PESHE in a manner most useful to the program and that best communicates to decision makers what ESOH issues affect the program. There is no specific format for the PESHE. At a minimum, the PESHE includes the following:

- Strategy for integrating ESOH considerations into the systems engineering process.
- Identification of who is responsible for implementing the ESOH strategy.
- Approach to identifying ESOH hazards and managing the associated risks.
- Approach for integrating ESOH hazard and associated risk information into the supportability strategy and/or fielding documentation.
- Specific risk matrix used by the program manager, with definitions for severity categories and probability levels, risk assessment values, risk categories, risk acceptance and user concurrence authorities, etc.
- Identification, assessment, mitigation, and acceptance of ESOH risks pursuant to DoD Instruction 5000.02, Enclosure 12, paragraph 6:

  Prior to exposing people, equipment, or the environment to known system-related ESOH hazards, the PM shall document that the associated risks have been accepted by the following acceptance authorities: the CAE for high risks, PEO-level for serious risks, and the PM for medium and low risks. The user representative shall be part of this process throughout the life cycle and shall provide formal concurrence prior to all serious- and high-risk acceptance decisions.

- Identification of the method for tracking hazards, mitigation measures, and associated risk assessment value throughout the life cycle of the system, and documenting the verified effectiveness of ESOH risk mitigation measures.
- Identify mitigation status for all hazards whose initial risk category is high or serious; for each hazard identify the following details: the initial, current, and target risk categories with risk assessment values; the hazard identification number, title, and description; and, mitigation(s), mitigation status and date.
- Compliance Schedule for the NEPA; Section 4321 et seq. of Title 42, United States Code, "National Environmental Policy Act;" and EO 12114, "Environmental Effects Abroad of Major Federal Actions" analyses and documentation.
- Identification of regulated hazardous materials (HAZMAT) (including energetics), wastes, materials of evolving regulatory interest (e.g., emerging contaminants), and

pollutants [discharges/emissions/noise (including personnel exposure to noise levels and potential noise impacts to communities near military facilities and ranges)] associated with the system and plans for their minimization and/or safe disposal. Program managers will need to collect, analyze, and possibly conduct specific tests to determine the estimated HAZMAT, waste, and pollutant associated with the system.

- Identification of applicable ESOH technology requirements incorporated into the system design.
- Approach for integrating HAZMAT, energetics, and other ESOH considerations (e.g., environmental impacts, personnel safety, regulatory compliance) into system demilitarization and disposal planning.
- A self-evaluation of the ESOH effort using the ESOH Management Evaluation Criteria for DoD Acquisition.
- The integration of ESOH and Human Systems Integration (HSI) and how the program avoids duplication between the HSI and ESOH efforts.
- Approach for integrating ESOH into test and evaluation (T&E) planning and reporting, as well as for providing safety releases prior to test activities.

  T&E planning shall consider the potential testing impacts on the environment [(42 U.S.C. 4321-4347 and EO 12114)].

  The PM, in concert with the user and the T&E community, shall provide safety releases (to include formal Environment, Safety, and Occupational Health (ESOH) risk acceptance in accordance with Section 6 of Enclosure 12) to the developmental and operational testers prior to any test using personnel.

Program managers should provide safety releases to the developmental and operational test organizations in accordance with component regulations. The program manager normally provides a safety release after conducting an appropriate hazard analysis and obtaining formal acceptance of identified ESOH risks expected to be present during testing.

DoD Instruction 5000.02 does not require that the PESHE supersede or replace other ESOH plans, analyses, and reports (e.g., System Safety Management Plan, HAZMAT Management Plan, Pollution Prevention Plan, System Safety Analyses, Health Hazard Assessments, etc.). The program manager incorporates these documents by reference, as appropriate. However, to the maximum extent possible, the program manager should minimize duplication of effort and documentation and give preference to recording ESOH information in the PESHE. HSI considerations (such as human factors, personnel habitability, and personnel survivability) at times interrelate with ESOH considerations. Program managers should ensure there is collaboration between these experts. HSI shares an interest in several safety and occupational health areas also addressed as part of the overall ESOH effort.

4.4.7.2. National Environmental Policy Act (NEPA)/Executive Order (EO) 12114 Compliance Schedule

The required NEPA/EO 12114, "Environmental Effects Abroad of Major Federal Actions" Compliance Schedule, presented in the Programmatic Environment, Safety, and Occupational Health Evaluation and summarized in the Acquisition Strategy, should include the following:

- Events or proposed actions (such as, but not limited to T&E and fielding/basing activities) throughout the life cycle of the program that may require preparation of formal NEPA/EO 12114 documentation;
- The anticipated initiation date for each proposed event or action;
- Proponent responsible for preparing the NEPA/EO 12114 documentation for each proposed event or action;
- The anticipated type of NEPA/EO 12114 document (e.g., Categorical Exclusion, Environmental Assessment and Finding of No Significant Impact, Environmental Impact Statement, Record of Decision, Overseas Environmental Assessment, and Overseas Environmental Impact Statement) which the proponent should complete prior to the proposed action start date;
- The anticipated start and completion dates for the final NEPA/EO 12114 document; and
- The specific approval authority for the documents. DoD Instruction 5000.02, E12.5.2, establishes the following:

  The CAE (or for joint programs, the CAE of the Lead Executive Component) or designee, [as] the approval authority for system-related NEPA and E.O. 12114 documentation.

4.4.7.3. Networks and Automated Information Systems (AIS)

Networks and AIS programs, including those using commercial off-the-shelf solutions, are not exempt from managing Environment, Safety, and Occupational Health (ESOH) compliance requirements as part of the systems engineering process. These systems are required to document those management efforts in a PESHE, as reflected in section 4.4.7.1. The AIS program manager should perform the ESOH analyses appropriate for the scope of the acquisition program (e.g., software; acquisition of hardware; installation of facilities, fiber optic cables, radio antennae, etc.). AIS programs that primarily deal with new or modified software applications should focus the PESHE on software system safety processes, procedures, and results. The PESHE for an AIS program that involves hardware and/or facilities should also address ESOH considerations such as man-machine interfaces, identification of HAZMAT, preparation of required NEPA/EO 12114 documentation, and demilitarization planning and disposal in accordance with security and HAZMAT/hazardous waste laws and regulations. All of the above factors, such as HAZMAT minimization, energy-efficiency, and human factors engineering/ergonomics, should be considered in the context of approaches to minimize life-cycle cost and risk and optimize process efficiency.

4.4.7.4. Environment, Safety, and Occupational Health (ESOH) Management Evaluation Criteria

DoD developed the "ESOH Management Evaluation Criteria for DoD Acquisition" to help Milestone Decision Authorities, Program Executive Offices, Program Support Review teams, and program managers assess implementation of ESOH policy and procedures throughout the acquisition phases and system's life cycle. The evaluation criteria are divided into the following four categories and are focused on assessing an acquisition program's overall management of ESOH considerations as an integral part of the systems engineering process:

- ESOH Planning;
- ESOH Hazard Identification, Analysis, and Risk Acceptance;
- ESOH Requirements for the System and Associated Infrastructure; and
- Personnel and Funding for ESOH.

Program managers should use these evaluation criteria to assess the implementation and effectiveness of the ESOH management process to influence system design and communicate risks to the user. The guide does not, however, assess the progress made in managing specific technical risks for identified ESOH hazards pursuant to MIL-STD-882D, "DoD Standard Practice for System Safety", but is an assessment of the overall ESOH effort.

4.4.7.5. Environment, Safety, and Occupational Health (ESOH) Risk Management

Balancing the elimination or reduction of ESOH risk with an informed and structured risk assessment and acceptance process is essential for positively contributing to a program's efforts in meeting the system's life-cycle cost, schedule, and performance requirements. The program manager should strive to eliminate or reduce ESOH risks as part of the system's total life-cycle risk reduction strategy. ESOH hazard and risk identification and implementation of effective mitigating measures is necessary to avoid loss of life or serious injury to personnel; serious damage to facilities or equipment; failures with adverse impact on mission capability, mission operability, or public opinion; and impact or harm to the environment and the surrounding community.

The ESOH risk management process uses ESOH risk analysis matrices, based on the requirements in MIL-STD-882D, "DoD Standard Practice for System Safety". The risk matrices shall define probability and severity criteria to categorize ESOH risks for identified ESOH hazards. In order to facilitate implementation of current DoD policy, the following definitions shall be used for ESOH risk management terminology:

- Causal Factor: One or several mechanisms that trigger the hazard.
- Hazard: A source or condition that if triggered by one or more causal factor(s) can contribute to or result in a mishap.
- Mishap: An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment (includes negative environmental impacts and accidents.

- Risk: (Hazard Risk). A measure of the potential loss from a given hazard. Risk is a combined expression of the severity of the mishap and the probability of the causal factor(s).
- Initial Risk: The first assessment of the potential risk of an identified hazard. Initial risk establishes a fixed baseline for the hazard.
- Current Risk: A measure of the risk from an identified hazard at a snapshot in time (e.g. at a program review).
- Event Risk: A measure of the risk from an identified hazard that applies only to the specified hardware/software configuration and event(s) of limited duration prior to fielding. Examples of events may include: testing, field user evaluation, and demonstrations.
- Target Risk: The anticipated residual risk assessment value and risk category of an identified hazard that the program manager plans to achieve by implementing mitigation measures consistent with the design order of precedence.
- Record of risk acceptance(s): The risk acceptance authority (and user concurrence authority, as applicable) by title and organization, date of acceptance, and location of the signed risk acceptance document; and,
- Residual Risk: The risk category of an identified hazard that remains after all mitigation measures have been implemented, verified, validated, and formally accepted prior to fielding. Complying with DoD accepted safety requirements in military standards, military specifications, Standardization Agreements or other related documents does not eliminate the residual risk.
- Mitigation measure: The recommended action required to eliminate the hazard or reduce the risk of one or more hazards by lowering the probability and/or severity of the mishap.

The three types of ESOH risks include:

- Impacts and adverse effects from routine system development, testing, training, operation, sustainment, maintenance, and demilitarization/disposal;
- Mission readiness impacts from system failures or mishaps, including critical software failures; and
- System life-cycle cost, schedule, and performance impacts from ESOH compliance requirements.

The scope of potential risks includes all ESOH regulatory compliance requirements associated with the system throughout its life cycle, such as, but not limited to, the following:

- Hazardous materials (HAZMAT) use and hazardous waste generation;
- Demilitarization and disposal requirements;
- Safety (including explosives safety, ionizing and non-ionizing radiation);
- Human health (associated with exposure to chemical, physical, biological, or ergonomic hazards, etc.);
- Environmental and occupational noise; and
- Impacts to the environment (e.g., air, water, soil, flora, fauna).

Programs should begin the process of identifying ESOH requirements and risks using lessons learned from the following sources of information:

- Legacy systems that the new system will replace, to include mishap and lost time rates associated with any legacy system;
- Similar systems;
- Pre-system acquisition activities (e.g., Analysis of Alternatives (AoA), Technology Development Strategy);
- Demilitarization and disposal of similar systems; and
- ESOH regulatory issues at potential locations for system testing, training, and fielding/basing.

The program manager is responsible for maintaining a closed-loop hazard tracking system to effectively track progress in managing ESOH risks throughout the life cycle of the system. The following information should be captured and maintained in the hazard tracking system:

- Hazard;
- Causal Factor(s);
- Mishap;
- Initial risk assessment value and risk category;
- Necessary mitigation measures to eliminate or reduce the risk;
- Target or residual risk assessment value and risk category;
- Hazard status (e.g., open, pending, closed);
- Hazard traceability (running history of actions taken or planned with rationale to mitigate risks through verification, validation, and acceptance);
- Action person(s) and organizational element;
- Risk acceptance authority (and user concurrence authority, as applicable) by title and organization, date of acceptance, and location of the signed risk acceptance document; and,
- Mitigation monitoring to measure effectiveness.

The system safety order of precedence for mitigating the risk from identified hazards starts from the most effective, preferred approach to the least effective, least preferred approach. The first option should always be to eliminate hazards through design selection and if unable to eliminate the hazard, then reduce the associated risk to acceptable levels through design selection. This option can reduce both the severity and probability of the risk. The remaining approaches can only reduce the probability of the associated risk. If an effort to use design selection has failed to eliminate the hazard or reduce the risk to acceptable levels, the program manager should then employ the less effective approaches. The next most effective option is to incorporate protective safety features or devices that do not require personnel response to reduce the risk to an acceptable level. If the ability to use these devices to adequately reduce the risk to acceptable levels is also restricted by other acquisition program considerations, then the program manager should employ detection and warning devices to alert personnel to the particular hazard and require some type of response. Only if the program manager is prevented from successfully

using the more effective options, should the least effective approach be employed of developing procedures (such as the use of personal protective equipment) and training to mitigate the risk to an acceptable level.

The program manager should monitor and assess the effectiveness of mitigation measures to determine whether additional controls are required. The program manager should document the status of progress made on implementing mitigation measures in the Programmatic ESOH Evaluation. Relevant information can include any related mishap data, adverse health effects, and environmental impacts from system development, testing, training, operation, sustainment, maintenance, and demilitarization/disposal. Programs should also convey information about the effectiveness of their risk management efforts with metrics, achievements, success stories, etc.

When the initial ESOH risk assessment identifies the HAZMAT either imbedded in the system or used for system operation and maintenance (to include energetics), additional risk information should be tracked as follows:

- The locations, quantities, and usage of HAZMAT in or on the system, where applicable;
- Safe demilitarization and disposal requirements;
- Energetic qualification information for each energetic material used in the system;
- Reasonably anticipated hazardous byproducts/discharges and expected quantities of hazardous waste generated during normal use/maintenance, in addition to those anticipated in emergency situations (e.g., exhaust, fibers from composite materials released during accidents, etc.);
- Special HAZMAT training, handling, and storage; and
- Assessment of risks associated with the expected use of any chemical or material that can be considered an emerging contaminant. Emerging contaminants are those that lack peer-reviewed toxicity values or regulatory standards, or the values and standards are evolving. The Emerging Contaminants Directorate in OSD maintains "watch" and "action" lists of emerging contaminants that pose possible or likely risks, respectively, to DoD functions. DoD maintains the lists on the Materials of Evolving Regulatory Interest Team (MERIT) web site, the official DoD source for emerging contaminants information. Program managers may be aware of additional emerging contaminants related to a specific acquisition program. Emerging contaminants have a high likelihood of coming under regulatory control, or more stringent regulatory control, and their continued use may pose increased risks to both mission and costs. Program managers should take action, as appropriate, to reduce these risks to acceptable levels.

The preferred mitigation strategy for HAZMAT risk management is source reduction or elimination of the hazards, also referred to as pollution prevention for dealing with potential environmental impacts. The program manager should strive to eliminate or reduce ESOH risks as part of the system's life-cycle risk reduction and total ownership cost (TOC) reduction strategies. The concept of TOC captures the true cost of design, development, ownership, and support of DoD weapons systems. To the extent that new systems can be designed to have lower ESOH risks (fewer mishaps) with no offsetting increase in the cost of the system or spares, the TOC for

these systems will be lower. The use of Business Case Analysis (BCA) during the evaluation of ESOH risk mitigation courses of actions, such as insertion of safety technologies or alternative system designs, can provide TOC benefits and support the program's overall TOC reduction strategy. For systems containing energetics, source reduction consists of minimizing the use of the energetic materials and developing system designs that reduce the possibility and consequences of an explosive mishap. This includes complying with the insensitive munitions criteria and pursuing hazard classifications and unexploded ordnance liabilities that minimize total ownership cost.

4.4.7.6. Environmental, Safety and Occupational Health (ESOH) Risk and Technology Requirements Reporting

Program managers are required to report the status of ESOH risk and acceptance decisions at technical reviews, such as System Requirements Review, Preliminary Design Review, Critical Design Review, and Test Readiness Reviews.

DoD Instruction 5000.02, Enclosure 12, paragraph 6, directs the following:

Program managers shall report on the status of ESOH risks and acceptance decisions at technical reviews. Acquisition program reviews and fielding decisions shall address the status of all high and serious risks, and applicable ESOH technology requirements.

Additionally, the Services are responsible for designating the user representative and ensuring they are included in the risk acceptance process. Chairman of the Joint Chiefs of Staff Instruction 3170.01 defines a "user representative" as "a command or agency that has been formally designated to represent single or multiple users in the capabilities and acquisition process. The Services and the Service components of the combatant commanders are normally the user representatives. There should only be one user representative for a system."

For acquisition program reviews and fielding decisions, the program manager should report the status of all high and serious risks and applicable safety technology requirements.

DoD Instruction 5000.02, Enclosure 12, paragraph 6, directs the following:

Acquisition program reviews and fielding decisions shall address the status of all high and serious risks, and applicable ESOH technology requirements.

The Deputy Under Secretary of Defense for Installations and Environment (DUSD(I&E)) developed the approach for providing the required ESOH risk and technology information to support program reviews and decisions (see section 4.4.7.5 for definitions). The reporting procedures for Acquisition Category (ACAT) ID and IAM programs are as follows:

- The program manager is expected to provide ESOH risk data to the office of the DUSD(I&E), Chemical and Material Risk Management Directorate at least two weeks

prior to any planned program review or fielding decision. Risk data should include all ESOH risks for which the current or target risk category is high or serious. The program manager should also include a report on all ESOH technologies required on the system and the implementation status of these technologies. For OSD-led program reviews and Fielding Decisions, provide the completed templates to the following email account: ESOH_Risk_Reporting@osd.mil.

- The program manager should report the ESOH risk data in the required format at the appropriate Integrated Product Team/Overarching Integrated Product Team and Executive Review Boards. The program manager should report the data using the format templates located on the Acquisition Community Connection's ESOH Special Interest Area Reporting ESOH Risk and Technology Requirements.

Each DoD Component is expected to implement a similar ESOH risks and safety technology status reporting process for ACAT IC, II, and III programs to meet the reporting requirements in DoD Instruction 5000.02.

In the event of a system-related Class A or B mishap, program managers are required to support the mishap investigation by providing analyses of hazards that contributed to the mishap and making recommendations for material risk mitigation measures, especially those that will minimize human error.

Program managers will support system-related Class A and B mishap investigations by providing analyses of hazards that contributed to the mishap and recommendations for materiel risk mitigation measures, especially those that minimize human errors.

4.4.7.7. Environmental, Safety and Occupational Health (ESOH) Risk Acceptance

Prior to exposing people, equipment, or the environment to known system-related ESOH hazards, the program manager should document the associated risks have been accepted by the following risk acceptance authorities: the Component Acquisition Executive for high risks, the Program Executive Office-level for serious risks, and the program manager for medium and low risks as defined in MIL-STD-882D, "DoD Standard Practice for System Safety." The user representative should be part of this process and provide formal concurrence prior to all high and serious risk acceptance decisions.

Typically, formal risk acceptances occur prior to specific events such as developmental and operational testing and fielding of prototypes to support urgent combat needs. In these cases, the risks to be accepted are for the hazards as configured in the system at that time and for the duration of the event (event risk). Formal risk acceptances also occur prior to fielding systems. The result is that a single hazard may require multiple formal acceptances as the system design evolves and events occur.

In addition, the risks associated with hazards discovered on systems after fielding should be formally accepted if the system is to remain in operation prior to full implementation of designated mitigation measures.

4.4.7.8. National Environmental Policy Act (NEPA)/ Executive Order (EO) 12114 Compliance Schedule Analysis

An effectively executed ESOH risk management effort also sets the stage for addressing NEPA/EO 12114 requirements by identifying system-specific ESOH risk information. The program manager combines system specific data with the known geographic/site specific environmental conditions and requirements, to prepare formal NEPA/EO 12114 analysis documents. Program managers are required to conduct and document NEPA/EO 12114 analyses, as well as other environmental compliance requirements (for example, regulatory agency consultations, permitting, etc.) for those actions which the program is the action proponent. In addition, the program manager is required to provide system specific data in support of NEPA/EO 12114 analysis to other action proponents. This approach may streamline the overall NEPA/EO 12114 analysis process, and possibly reduce cost and schedule impacts. The program manager should integrate into the ESOH risk management data any additional ESOH risks or additional mitigation measures identified during the NEPA/EO 12114 analysis process.

DoD Instruction 5000.02states the following:

The PM shall conduct and document NEPA/E.O. 12114 analyses for which the PM is the action proponent. The PM shall provide system-specific analyses and data to support other organizations' NEPA and E.O. 12114 analyses. The CAE (or for joint programs, the CAE of the Lead Executive Component) or designee, is the approval authority for system-related NEPA and E.O. 12114 documentation.

4.4.7.9. Unmanned Systems (UMS)

Because UMS and unmanned variants of manned systems are being rapidly developed and fielded to meet critical warfighter capability needs, Deputy Under Secretary of Defense for Installations and Environment/Environmental Readiness and Safety and Deputy Under Secretary of Defense for Acquisition &Technology/Systems Engineering developed the "Unmanned Systems Safety Guide for DoD Acquisition." This guide is designed to assist program managers and chief engineers in their efforts to ensure that system safety and Environmental, Safety and Occupational Health (ESOH) considerations are included in the development and fielding of UMS. Program Managers for UMS and unmanned variants of manned systems should address at Critical Design Review and in the Programmatic ESOH Evaluation (PESHE) consistency with the applicable programmatic, operational, and design precepts defined in the Guide.

4.4.7.10. Green Procurement

Program managers should consider green products and services as part of systems engineering and the Programmatic Environment, Safety, and Occupational Health (ESOH) Evaluation (PESHE). Executive Order (EO) 13423, "Strengthening Federal Environmental, Energy, and Transportation Management," requires Federal agencies to increase their energy efficiency by purchasing biobased, recycled content, energy-efficient, water-efficient, and environmentally preferable products; reducing greenhouse gases; reducing the amount of petroleum products used; and reducing the quantity of toxic chemicals and HAZMAT purchased. Program managers should monitor the following considerations throughout the life cycle of the system:

- Procure products (such as computers and monitors) with Energy Star® features and energy efficient standby power devices.
- Expand procurement of environmentally sound, "green" products (energy and water efficient, recycled content, etc.) including consideration of biobased products.
- Reduce energy consumption of system components, when possible. Program managers should consider the fully burdened cost of delivered energy for tactical systems.
- Track all toxic chemicals and hazardous materials used and when possible replace or reduce the use of these materials including the generation of solid waste, the use of volatile organic compounds, and not using ozone depleting substances.
- Reuse, donate, sell, or recycle electronic products using environmentally sound management practices. Such consideration should be included as part of overall demilitarization and disposal planning for the acquisition system.

Additional direction on EO 13423 is provided in "Instructions for Implementing Executive Order 13423."

4.4.7.11. Software System Safety

Since the development of the digital computer, software continues to play an important and evolutionary role in the operation and control of hazardous, safety-critical functions. Human control of hazardous operations has diminished dramatically in the last 15 years. Today, digital computer systems have autonomous control over safety-critical functions in nearly every major technology, both commercially and within government systems. This revolution is primarily due to the ability of software to reliably perform critical control tasks at speeds unmatched by its human counterpart. Other factors influencing this transition is our ever-growing need and desire for increased versatility, greater performance capability, higher efficiency, and a decreased life cycle cost. In most instances, software can meet all of the above attributes of the system's performance when properly designed. The logic of the software allows for decisions to be implemented without emotion, and with speed and accuracy. This has forced the human operator out of the control loop; because they can no longer keep pace with the speed, cost effectiveness, and decision making process of the system.

Therefore, there is a critical need to perform system safety engineering tasks on safety-critical systems to reduce the safety risk in all aspects of a program. These tasks include the software system safety (SSS) activities involving the design, code, test, Independent Verification and

Validation (IV&V), operation & maintenance, and change control functions of the software engineering development process. The Joint Software System Safety Committee's Software System Safety Handbook https://nossa.nmci.navy.mil/extensions/wise/documents/SoftwareSystemSafetyHandbook.pdf provides management and engineering guidelines to achieve a reasonable level of assurance that software will execute within the system context with an acceptable level of safety risk.

4.4.8. Human Systems Integration (HSI)

From DoD Directive 5000.01, E1.1.29:

The program manager shall apply human systems integration to optimize total system performance (hardware, software, and human), operational effectiveness, and suitability, survivability, safety, and affordability.

And from DoD Instruction 5000.02, Enclosure 8, paragraph 1:

The PM shall have a plan for HSI in place early in the acquisition process to optimize total system performance, minimize total ownership costs, and ensure that the system is built to accommodate the characteristics of the user population that will operate, maintain, and support the system.

The program manager shall apply HSI to optimize total system performance and minimize total ownership cost. It may be necessary for the program manager to estimate long-term savings in manpower, personnel, training, or operations and support costs to justify potential increases in design and acquisition costs.

To do this, the program manager will work with the manpower, personnel, training, safety, and occupational health, environment, habitability, survivability, and human factors engineering communities to translate and integrate the HSI thresholds and objectives contained in the capabilities documents into quantifiable and measurable system requirements. The program manager then includes these requirements in specifications, the Test and Evaluation Master Plan, and other program documentation, as appropriate, and uses them to address HSI in the statement of work and contract. The program manager identifies any HSI-related schedule or cost issues that could adversely impact program execution; the system's support strategy should identify responsibilities, describe the technical and management approach for meeting HSI requirements, and summarize major elements of the associated training system. See also MIL-STD-1472F, Human Engineering (scroll down and select "Revision F"). HSI topics include:

- Human Factors Engineering (DoD Instruction 5000.02 and Guidebook section 6.3.4),
- Habitability and Personnel Survivability (DoD Instruction 5000.02 and Guidebook sections 4.4.13, 6.3.7, and 6.3.6),
- Manpower Initiatives (DoD Instruction 5000.02 and Guidebook section 6.3.1),
- Personnel Initiatives (DoD Instruction 5000.02 and Guidebook section 6.3.2), and

- Training (DoD Instruction 5000.02 and Guidebook section 6.3.3).

4.4.9. Insensitive Munitions (IM)

10 U.S.C. 2389 tasks the Secretary of Defense to ensure, to the extent practicable, that IM under development or procurement are safe throughout development and fielding when subject to unplanned stimuli. IM are those that reliably fulfill their performance, readiness, and operational requirements on demand, and that minimize the probability of inadvertent initiation and the severity of subsequent collateral damage to weapon platforms, logistic systems, and personnel when subjected to selected accidental and combat threats.

Each Program Executive Office (PEO) is required to submit for Joint Requirements Oversight Council (JROC) approval a biennial IM Strategic Plan that provides the Office of the Under Secretary of Defense (Acquisition, Technology, and Logistics (OUSD(AT&L)) and the JROC increased visibility into the total PEO munitions portfolio, their IM efforts, and investment priorities. The IM Strategic Plans serve as a roadmap for how each PEO plans to achieve an IM compliant munitions portfolio and identifies the gaps (funding, technology, etc) which prevent them from achieving this goal.

A single standardized set of IM tests and passing criteria (see Table 4.4.9.T1) are to be used by all Components for evaluating and reporting on the IM compliance status of the munitions in their portfolio. These standards are the default for use for typical munitions programs. For atypical circumstances, deviations will require review and approval by the JROC through the Joint Capabilities Integration and Development System (JCIDS).

TEST	THREAT	PASSING CRITERIA	CONFIGURATION
FAST COOK-OFF*	Liquid Fuel Fire	Type V Burning	1 Tactical 1 Logistical
SLOW COOK-OFF*	Slow Heating 3.3° C/HR	Type V Burning	2 Logistical
BULLET IMPACT*	.50 Cal M2AP 3 Round Burst	Type V Burning	1 Tactical 1 Logistical
FRAGMENT IMPACT	STANAG 4496 Fragment 8300 ft/sec	Type V Burning	1 Tactical 1 Logistical
SHAPED CHARGE	81mm	Type III	1 Tactical

JET IMPACT	Precision Shaped Charge	Explosion	1 Logistical
SYMPATHETIC REACTION*	Detonation of an adjacent munition	Type III Explosion	2 Logistical - 1 Confined, 1 Unconfined 1 Donor & 2 Acceptors per Test

* REQUIRED FOR 1.2.3 AND 1.6 HAZARD CLASSIFICATION ASSIGNMENTS

Table 4.4.9.T1. IM tests and Passing Criteria

The single standardized IM tests are harmonized with the tests required to obtain more favorable hazard classifications, thus ensuring that success with IM compliance translates to reductions or avoidances in life-cycle cost.

All submunitions and submunition-containing weapons, regardless of ACAT, should conform to the policy of reducing overall unexploded ordnance through a process of improving the submunitions system reliability—the desire is to field future submunitions with a 99 percent or higher functioning rate (SecDef Memorandum, 10 Jan 01, subject: DoD Policy on Submunition Reliability). The JROC will approve any waivers of this policy for Acquisition Category I and II submunition weapons programs.

4.4.10. Interoperability

All acquisition programs are required to address satisfactorily interoperability and integration. These requirements span the complete acquisition life cycle for all acquisition programs. Interoperability and supportability of information technology and National Security System (NSS) acquisition programs are required to comply with DoD Directive 4630.05, DoD Instruction 4630.8, CJCS Instruction 3170.01, the JCIDS Manual, CJCS Instruction 6212.01, Public Law 104-106 and 44 U.S.C. 3506.

4.4.11. Open Systems Design

DoD Instruction 5000.02, Enclosure 12, paragraph 8, directs the use of open systems design across the acquisition life cycle per the following extract:

Program managers shall employ a Modular Open Systems Approach (MOSA) to design for affordable change, enable evolutionary acquisition, and rapidly field affordable systems that are interoperable in the joint battle space.

MOSA is an integrated business and technical strategy for assessment and implementation of open systems in the DoD. An open system is a system that employs modular design tenets, uses widely supported and consensus-based standards for its key interfaces, and is subject to validation and verification, including test and evaluation, to ensure the openness of its key interfaces. An open systems design is a design approach for developing an affordable and adaptable open system. It derives inputs from both the technical management processes and technical processes undertaken within the systems engineering and other life-cycle processes, and in turn impacts these processes. The open systems design strategy should be implemented as part of the program's overall technical approach and becomes an integral part of the program's Systems Engineering Plan.

A key enabler in the design of open systems is the use of open standards. The DoD Information Technology Standards Registry mandates the minimum set of standards and guidelines for the acquisition of all DoD systems that produce, use, or exchange information.

Program managers should employ an open systems design strategy only after careful analysis of required capabilities and strategies for technology development, acquisition, test and evaluation, and product support. They should also analyze the effects of information assurance, systems safety and security, Commercial-off-the-shelf availability, and other design considerations before finalizing their open systems design strategy. For example, programs should ensure that required capabilities lend themselves to the application of open systems design and do not impose premature design-specific solutions. Program managers should also evaluate the appropriateness of an open systems design in light of environmental constraints such as very high temperature, excessive humidity, and safety and security needs of the system. The bottom line is that program managers should make a business case for using the open systems design through the application of trade studies, dynamic cost models, and market research aimed at analyzing technology and open standard trends and the degree of market support for needed technologies and standards.

All programs subject to milestone review should document their MOSA and include a summary in the program Acquisition Strategy and SEP. Programs should report their MOSA implementation progress through Program Support Reviews (PSR). Before a PSR, program managers can conduct a self-assessment of their MOSA implementation using MOSA Program Assessment and Review Tool. Program managers should employ an open systems design strategy within the context of implementing their overall plan for MOSA implementation. Programs should comply with the "Program Manager's Guide: A Modular Open Systems Approach (MOSA) to Weapon System Acquisition." Programs not complying with the guidelines should provide justification or a migration plan to the PSR office for achieving compliance.

Within the MOSA context, programs should design their system based on adherence to the following five MOSA principles:

- Establish an Enabling Environment. This principle lays the foundation for successful implementation of subsequent principles. To adhere to this principle, the program

manager establishes supportive requirements, business practices, and technology development, acquisition, test and evaluation, and product support strategies needed for effective development of open systems. Assigning responsibility for MOSA implementation, ensuring appropriate experience and training on MOSA, continuing market research, and proactive identification and overcoming of barriers or obstacles that can potentially slow down or even, in some cases, undermine effective MOSA implementation are among the supportive practices needed for creating an enabling MOSA environment.

- Employ Modular Design. Effective modular design is contingent upon adherence to four major modular design tenets. These tenets determine the degree to which modules are cohesive (contain well-focused and well-defined functionality); encapsulated (hide the internal workings of a module's behavior and its data); self-contained (do not constrain other modules); and highly binned (use broad modular definitions to enable commonality and reuse). By following these tenets, each module will be designed for change and the interface to each module is defined in such a way as to reveal as little as possible about its inner workings that facilitate the standardization of modular interfaces.
- Designate Key Interfaces. To effectively manage hundreds, and in some cases thousands, of interfaces that exist within and among systems, designers should group interfaces into key and non-key interfaces. Such distinction enables designers and configuration managers to distinguish among interfaces that exist between technologically stable and volatile modules, between highly reliable and more frequently failing modules, between modules that are essential for net-centricity and those that do not perform net-centric functions, and between modules that pass vital interoperability information and those with least interoperability impact.
- Use Open Standards. To take full advantage of modularity in design, interface standards should be well defined, mature, widely used, and readily available. Moreover, standards should be selected based on maturity, market acceptance, and allowance for future technology insertion. As a general rule, preference is given to the use of open interface standards first, the de facto interface standards second, and finally government and proprietary interface standards. Basing design strategies on widely supported open standards increases the chance that future changes will be able to be integrated in a cost effective manner.
- Certify Conformance. Openness of systems is verified, validated, and ensured through rigorous and well-established assessment mechanisms, well-defined interface control and management, and proactive conformance testing. The program manager, in coordination with the user, should prepare validation and verification mechanisms such as conformance certification and test plans to ensure that the system and its component modules conform to the external and internal open interface standards allowing plug-and-play of modules, net-centric information exchange, and re-configuration of mission capability in response to new threats and evolving technologies. Open systems verification and validation should become an integral part of the overall organization's configuration management processes. The verification and validation should also ensure that the system components and selected commercial products avoid utilization of vendor-unique extensions to interface standards and can easily be substituted with similar

components from competitive sources. Program managers should either use their own tool or preferably the MOSA Program Assessment and Review Tool, to assess the compliance with open systems policies and ensure that their programs are properly positioned to reap the open systems benefits.

Adherence to these principles ensures access to the latest technologies and products, achieve interoperability, and facilitate affordable and supportable modernization of fielded assets. Such adherence ensures delivery of technologically superior, sustainable and affordable increments of militarily useful capability within an evolutionary acquisition strategy context. For more information and detailed guidance on using MOSA and open systems design, see Chapter 2, section 2.3.1.1 and review the Program Manager's Guide, discussed above.

4.4.12. Parts Management

Parts management is a design strategy that seeks to reduce the number of unique or specialized parts used in a system (or across systems) to reduce the logistic footprint and lower total life-cycle costs. In addition, it also will enhance the reliability of the system and mitigate parts obsolescence because of Diminishing Manufacturing Sources and Material Shortages. Parts management is an important design consideration and should be used whenever parts are not defined based on open systems design interfaces or Commercial-off-the-shelf items, as described in sections 4.4.6 and 4.4.2, respectively.

A part is one piece, or two or more pieces joined together, that is not normally subject to disassembly without destruction or impairment of intended design use. A part is the lowest configuration item of the system design that would be implemented and verified. Parts are defined in performance-based terms by their form, fit, function, and interfaces.

The parts management strategy should cover the entire life cycle of a system and be based on the fundamental systems engineering processes described in sections 4.2.3 and 4.2.4. The parts management strategy should also be evaluated at technical reviews, in particular, the Preliminary Design Review and Critical Design Review. The Systems Engineering Plan should address the parts management strategy, including the need for a parts management plan as defined in MIL-STD-3018. A parts management plan typically includes the following:

- Specification of parts selection criteria based on objectives in the Acquisition Strategy Report and overall support strategy,
- Identification of a preferred parts list,
- Definition of the processes for conducting trade-off analysis, parts selection, inclusion of configuration identification status and related change decisions in the technical baseline, and approval and documentation of non-preferred parts, and
- Discussion of how parts management considerations will flow down to suppliers.

Parts selection should be based on trade-off and cost-benefit analyses that are conducted in accordance with the program's parts strategy and management plan, as derived from the overall

acquisition and sustainment strategies. Selected parts should be documented in a parts list, which is under configuration management of the overall technical baseline.

See MIL-STD-3018, "Parts Management," SD-19, "Life-cycle Cost Savings Through Parts Management," and related industry specifications, such as AIA and ANSI/AIAA-R-100 (available for purchase) and ANSI/EIA-4899 (available for purchase) for more details on recommended parts management practices. "Reduce Program Costs through Parts Management" provides details for conducting a business case for having a Parts Management Program. Additional information on DoD Parts Management is available on the Defense Standardization Program Office website and the Parts Standardization & Management Committee website.

4.4.13. Program Protection & System Assurance

4.4.13. Program Protection & System Assurance

Program protection is the process for protecting "Acquisition Programs." It is the responsibility of the program manager to ensure that:

Pre-Milestone A:

- A draft list of Critical Program Information is developed, and
- A summary of and status on the Program Protection Plan (PPP) is included within the Acquisition Strategy.

Pre-Milestone B:

- Program protection requirements are included in the Request For Proposal, and
- A PPP is written and submitted to the Milestone Decision Authority (MDA).

Pre-Milestone C:

- Program protection requirements are met by the contractor.

The MDA is the approval authority for the PPP and the Acquisition Strategy that is developed by the program manager.

4.4.13.1. Program Protection Planning

Program protection planning is the process of identifying Critical Program Information (CPI) and determining countermeasures needed to safeguard the CPI throughout the acquisition process. It is DoD policy to identify CPI early in the technology development phase. Effective program protection planning depends on a process of identifying CPI and applying the appropriate awareness and safeguarding actions.

All DoD acquisition programs are to be reviewed by the program manager (or the responsible commander/manager if a program manager has not been appointed) to determine if the program contains CPI.

To facilitate the review of their programs, the program manager, with the assistance of a working-level integrated products team (WIPT), identify CPI. It is the responsibility of the program manager to ensure that the WIPT is comprised of appropriate representatives.

After the identification of CPI, the program manager documents this action in a Program Protection Plan (PPP). With the assistance of Counterintelligence, Security, Intelligence, Anti-Tamper and systems engineering support activities, ensure implementation of countermeasures to protect all CPI identified during the CPI assessment.

Not all acquisition programs will contain CPI. If the program manager determines that there is no CPI, this determination, and the process used to make that determination, shall be documented by a Program Protection Plan (PPP) for concurrence by the appropriate level Program Executive Officer, Service Acquisition Executive, or Milestone Decision Authority. Additional information on PPP can be found in Chapter 8.

4.4.13.2. Critical Program Information (CPI)

The Program Protection Plan (PPP) is a risk-based, comprehensive, living plan to protect CPI that is associated with a research, development, and acquisition program. The PPP is used to develop tailored protection guidance for dissemination and implementation throughout the program for which it is created. The layering and integration of the selected protection requirements documented in a PPP provide for the integration and synchronization of CPI protection activities throughout the Department of Defense. Threats to CPI, vulnerabilities of CPI, and risk mitigation countermeasures are contained with the PPP.

4.4.13.3. Threats, Vulnerabilities, Risk Assessment

DoD Instruction 5200.39 defines Critical Program Information as elements or components of an research, development, and acquisition program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability; It includes information about applications, capabilities, processes, and end-items; Includes elements or components

critical to a military system or network mission effectiveness; Includes technology that would reduce the US technological advantage if it came under foreign control.

CPI information shall be identified early in the research, technology development and acquisition processes, but no later than when a DoD Agency or military component demonstrates an application for the technology in an operational setting, in support of a transition agreement with a pre-systems acquisition or acquisition program, or in exceptional cases, at the discretion of the laboratory/technical director.

Pre-systems acquisition and acquisition programs shall review their programs for CPI when technologies are transitioned from research and development or inherited from another program, during the Technology Development phase, throughout program progression, and as directed by the Milestone Decision Authority.

4.4.14. Quality and Producibility

4.4.14.1. Quality in Design

Design engineering efforts should lead to a producible and testable product. The objectives of these design efforts are to achieve effective and efficient manufacturing processes with the necessary process controls to satisfy requirements and minimize manufacturing costs. The design of the system should facilitate, throughout the supply chain, the timely and affordable manufacture, assembly, and delivery of a quality product to the customer.

Process capability is measured by the reproducibility of the products created from the process, where reproducibility is defined by the extent of variation in characteristics among the products. When there is a high degree of product uniformity, the process is said to be in statistical control. Process capability goes beyond machine capability. It also includes the effects of changes in workers, materials, fabrication methods, tooling and equipment, set-up, and other process conditions. Process capability data should be collected throughout development. While early data collection efforts may rely on opinion or small sample size, the data should be continuously refined using test articles and eventually, production.

A process may be in control without the product's characteristics being within specification limits. Therefore, to achieve high quality (product characteristics are within specification limits as necessary to satisfy customer requirements and enhance customer satisfaction), the product should be designed such that the:

- Process to produce it can be in statistical control over an extended period of time and varying conditions, and
- Design specifications are aligned with manufacturing process capabilities.
- Some tools used to support process characterization and variation management are discussed below.

Six Sigma techniques identify and reduce all sources of product variation – machines, materials, methods, measurement systems, the environment, and the people in the process. They are aimed at achieving virtually defect-free operations (99.99966 percent perfection or 3.4 defects per million opportunities), where parts or components can be built to very exacting performance specifications. Six Sigma can be characterized as a data driven approach to continuous process improvement.

The basic steps of a Six Sigma improvement process may be characterized as follows:

- **Define**: Define customer requirements and develop a map of the process to be improved,
- **Measure**: Identify key measures of effectiveness and efficiency and translate them into the concept of sigma,
- **Analyze**: Analyze the causes of the problem requiring improvement,
- **Improve**: Generate, select, and implement solutions, and
- **Control**: Ensure that improvement is sustained over time.

A good experimental design is an important prerequisite for the "analyze" step. A design of experiment is an organized approach for determining the relationship between factors affecting a process and the output of that process. The experiments will systematically vary all pertinent factors to determine those factor values that "improve" the output.

Quality Function Deployment (QFD) is another useful tool. QFD is a structured approach to understanding customer requirements and translating them into products that satisfy those needs. It uses a series of matrices in a four step approach as described below:

- Define and prioritize customer requirements and plan a product that responds to those needs,
- Develop product specifications using relationships between requirements and critical characteristics,
- Design the production process such that the process capability is sufficient for the customer needs, and
- Establish process controls to ensure critical characteristics (i.e., those characteristics most essential for success) are within the specification limits.

The need to design parts that are easy to produce should be balanced against the need to design parts that are easy to assemble. Design considerations in the latter area include part count, accessibility, packaging, modularity, use of standardized parts, and installation orientation and complexity.

4.4.14.2. Manufacturing Readiness

The program manager should use existing manufacturing processes whenever possible. When the design requires new manufacturing capabilities, the program manager needs to consider process flexibility (e.g., rate and configuration insensitivity). Full-Rate Production of a system necessitates a stable design, proven manufacturing processes, and available or programmed production facilities and equipment (see the Production Readiness Review for additional information).

Manufacturing readiness is a measure of producibility. It is the ability to harness the manufacturing, production, quality assurance, and industrial functions to achieve an operational capability that satisfies mission needs in the quantity and quality needed by the war-fighter to carry out assigned missions at the "best value" as measured by the warfighter. Best value refers to increased performance as well as reduced cost for developing, producing, acquiring, and operating systems throughout their life cycle. Manufacturing readiness begins before, continues during the development of systems, and even after a system has been in the field for a number of years.

Assessment of Manufacturing Readiness involves continuous assessments performed throughout the acquisition process and in conjunction with the systems engineering technical reviews that specifically measure manufacturing readiness from the Materiel Solution Analysis phase all the way through the Production and Deployment phase. The assessments focus on identifying and mitigating manufacturing risk and ensuring a program or technology is ready to move forward based on a manufacturing perspective.

Manufacturing Readiness Levels (MRLs) are used with assessments and are designed to assess the maturity of a given technology, system, subsystem, or component from a manufacturing prospective. MRLs provide decision makers (at all levels) with a common understanding of the relative maturity (and attendant risks) associated with manufacturing technologies, products, and processes being considered to meet DoD requirements.

Manufacturing Readiness Levels (MRLs) are designed to assess the maturity of a given technology, system, subsystem, or component from a manufacturing prospective. MTLs provide decision makers (at all levels) with a common understanding of the relative maturity (and attendant risks) associated with manufacturing technologies, products, and processes being considered to meet DoD requirements.

4.4.15. Reliability, Availability, and Maintainability

Reliability, availability and maintainability (RAM) have a direct impact on both operational capability and total ownership costs (TOC), and therefore are important considerations for the warfighter. Achieving required levels of RAM for a system is important for many reasons, some of which are identified below:

- Improved readiness—Readiness is the state of preparedness of forces or systems to meet a mission, based on adequate and trained personnel, material condition, supplies/reserves of support systems and ammunition, numbers of units available, etc. Poor reliability or maintainability causes readiness to fall below needed levels or increases the cost of achieving them.
- Improved safety—Inadequate reliability of components deemed Critical Safety Items (CSIs) may directly jeopardize the safety of the user(s) of that component's system and result in a loss of life. The ability to complete a mission safely is directly related to the reliability of the CSIs.
- Improved mission success—Inadequate reliability of equipment directly jeopardizes mission success and may result in undesirable repetition of the mission. The ability to complete a mission successfully is directly affected by the extent to which equipment needed to perform a given mission is available and operating properly when needed.
- Reduced TOC—The concept of TOC captures the true cost of design, development, ownership, and support of DoD weapons systems. To the extent that new systems can be designed to be more reliable (fewer failures) and more maintainable (fewer resources needed) with no offsetting increase in the cost of the system or spares, the TOC for these systems will be lower.
- Reduced logistics footprint—The logistics footprint of a system consists of the number of logistics personnel and the materiel needed in a given theater of operations. The ability of a military force to deploy to meet a crisis or move quickly from one area to another is determined in large measure by the amount of logistics assets needed to support that force. Improved RAM reduces the size of the logistics footprint related to the number of required spares, maintenance personnel, and support equipment. This has the additional benefit of reducing energy or other natural resource consumption and may help to reduce hazardous materials.
- Improved Maintainability—Designing the system and maintenance procedures so that maintenance can be performed quickly, easily, and cost-effectively.

Many factors are important to RAM: system design, manufacturing quality, the environment in which the system is transported, handled, stored, and operated; the design and development of the support system; the level of training and skills of the people operating and maintaining the system; the availability of materiel required to repair the system; and the diagnostic aids and tools (instrumentation) available to them. All these factors should be well understood to achieve a system with a desired level of RAM.

Reliable, available and maintainable systems are achieved through a disciplined systems engineering approach employing the best design, manufacturing, and support practices. To achieve the user's RAM requirements, emphasis should be on the following:

- Understanding the user's system readiness and mission performance requirements, physical environments (during use, maintenance, storage, transportation, etc.), the resources (people, infrastructure, dollars, etc.) available to support the mission, the risks

associated with these requirements, and translating them into system requirements that can be implemented in the design and verified,
- Managing the contributions to system RAM that are made by hardware, software, and human elements of the system,
- Identifying potential failure mechanisms and making design changes to remove them, precluding the selection of unsuitable parts and materials, and minimizing the effects of variability in the manufacturing and support processes, and
- Developing robust systems, insensitive to the environments experienced throughout the system's life cycle and capable of being repaired under adverse or challenging conditions.

Some RAM pitfalls to avoid when executing a sound systems engineering process include:

- Arbitrary user RAM requirements that may not be achievable or cost effective,
- Failure to identify mission context or intended use profile when stating RAM requirements,
- Failure to take into account the stochastic character of RAM and hence suitably consider statistical confidence issues,
- Inadequate planning for reliability and maintainability,
- Failure to design-in reliability early,
- Reliance on predictions instead of design analyses,
- Timing and execution of RAM related tasks not synchronized with the design process
- Failure to perform engineering analyses of Commercial-Off-the-Shelf equipment,
- Inadequate quality management and timeliness of root cause analysis and corrective actions,
- Inadequate lower level testing,
- Lack of proper planning, managing, and executing reliability growth activities,
- Arbitrary interpretations of failure or system use during testing,
- Lack of reliability incentives, and
- Failure to identify producibility issues as part of the development effort.

RAM are key characteristics of any effective system. They affect our ability to undertake and successfully execute a mission. Their influence on total ownership cost is significant. The ability of our fighting forces to deploy to meet a crisis or move quickly from one area to another and the safety of those fighting forces is dependent on having reliable and maintainable systems.

It is department policy for programs to be formulated to execute a viable RAM strategy that includes a reliability growth program. Relevant guidance can be found in the "DoD Guide for Achieving Reliability, Availability, and Maintainability." Further, the reliability growth program should be an integral part of design and development and should be integrated within the systems engineering processes. Use of GEIA-STD-0009, "Reliability Program Standard for Systems Design, Development, and Manufacturing" (available for sale), and associated contractual language will ensure this occurs. The reliability scorecard can be used to evaluate the developer's reliability practices. RAM program should be documented in the program's Systems Engineering

Plan and Life-cycle Sustainment Plan, and assessed during technical reviews, test and evaluation, and Program Support Reviews.

Additional RAM guidance can be found in the Reliability and Maintainability Continuous Learning Module (CLE301) at the Defense Acquisition University (DAU) Virtual Campus Learning Center and at the DAU Acquisition Community Connection (ACC) website, in the Reliability, Availability, and Maintainability Special Interest Area.

4.4.16. Software

The following best practices for software systems also apply in general to any system:

- Viewing the software "content," particularly complex algorithms and functional flows, as enabling technologies requiring maturation and risk reduction before Milestone B,
- Developing architectural-based software systems that support open system concepts,
- Exploiting commercial, off-the-shelf (COTS) computer systems products,
- Allowing incremental improvements based on modular, reusable, extensible software,
- Identifying and exploiting, where practicable, government and commercial software reuse opportunities before developing new software,
- Selecting the programming language in context of the systems and software engineering factors that influence system performance, overall life-cycle costs, risks, and the potential for interoperability,
- Using DoD standard data and following data administrative policies in DoD Directive 8320.02,
- Selecting contractors with domain experience in developing comparable software systems, successful past performance, and demonstrated commitment to disciplined software development process.
- Assessing information operations risks (see DoD Directive 3600.01) using techniques such as Program Support Reviews,
- Preparing for life-cycle software support or maintenance by planning early in the system life cycle for the transition of fielded software to the support/maintenance activity, developing or acquiring the necessary documentation, host systems, test beds, and computer-aided software engineering tools consistent with planned support concepts,
- Tracking COTS software purchases and maintenance licenses, and
- Performing system safety engineering tasks on safety-critical systems to reduce the safety risk in all aspects of a program, including the software system safety (SSS) activities involving the design, code, test, Independent Verification and Validation (IV&V), operation & maintenance, and change control functions of the software engineering development process.

The program manager should structure a software development process to recognize that emerging capabilities and missions will require modification to software over the life cycle of the system. To deliver truly state-of-the-software, this process should allow for periodic software enhancements.

Non-Developmental Software (NDS) is any software that is not legacy software for the program, or is not developed as part of the effort being accomplished by the developer team. NDS includes COTS software, government furnished software, open source software, and software being reused from another program. NDS can provide significant benefits including faster delivery of capabilities, reduced costs, and faster technology upgrades. NDS can also introduce numerous risks to the program that can have contractual and long-term sustainment implications. Robust systems engineering is essential for developing a system using NDS.

The use of COTS software brings additional challenges. Development, delivery and upgrades of COTS products are market-driven. Control of the future direction of the component is surrendered. Modifying COTS software is strongly discouraged, as the resulting component is no longer a COTS product. Although security and assurance are important considerations for all software activities, they are critical for COTS products, which may have been developed outside the normal trusted supplier base that is subject to industrial security requirements. When contemplating the use of NDS software, consider the following:

- Ensure decisions to use NDS are based on and are traceable to validated system architecture and design requirements.
- Include appropriate NDS activities in the program Integrated Master Plan/Integrated Master Schedule.
- Evaluate all proposed NDS to the extent possible at the start of the development
- Establish configuration control procedures to address NDS integration, upgrades, and changes throughout the system life cycle.
- Assess suitability and manage technical risk inherent in NDS during the system development phase.
- Address security/assurance concerns with COTS software.
- Track COTS software purchases and maintenance licenses.
- Carefully evaluate for realism offerors proposals that include significant amounts of software re-use.

The Open Source Initiative (OSI) contains more information on open source and open source licenses. The OSI is a non-profit corporation which maintains the complete Open Source Definition consisting of ten requirements which software should meet to be considered open source, and the OSI license review process which, through a public review process, ensures that licenses and software labeled as "open source" comply with the Open Source Definition and conform to existing community norms and expectations." However, this does not guarantee reliability, safety, or security.

Additionally, the program manager should apply the following security considerations to software design and management:

- A documented impact analysis statement that addresses software reliability, additional functionality in NDS, and accompanies modifications to existing DoD software,
- Formal software change control processes,

    - Software quality assurance personnel monitor the software change process, and
    - An independent verification and validation team provides additional review.
- Analysis of the technical risks and vulnerabilities of the software that could be exploited, with identified mitigation strategies,
- A change control process indicating whether foreign nationals, in any way, participated in software development, modification, or remediation,
- Security clearance for each foreign national employed by contractors/subcontractors to develop, modify, or remediate software code specifically for DoD use, commensurate with the level of the program in which the software is being used,
- Assurance that primary vendors on DoD contracts that have subcontractors who employ cleared foreign nationals work only in a certified or accredited environment (DoD Instruction 8510.01),
- Review of DoD software for malicious code by software quality assurance personnel for coding done in foreign environments or by foreign nationals,
- Preference to vendors who can demonstrate efforts taken to minimize the security risks associated with foreign nationals who developed, modified, or remediated the COTS software being offered during product selection and evaluation
- Review by software quality assurance personnel of software sent to locations not directly controlled by the DoD or its contractors for malicious code when it is returned to the DoD contractor's facilities.

4.4.17. Spectrum Management

Per DoD Instruction 5000.02, Enclosure 12, paragraph 11:

For all electromagnetic spectrum-dependent systems, PMs shall comply with U.S. and host nation spectrum regulations. They shall submit written determination to the DoD Component CIO or equivalent that the electronic spectrum necessary to support the operation of the system during its expected life cycle, or will be, available [DoD Directive 4650.1].

Spectrum Management is an important systems design consideration with mandatory requirements for each milestone reviews as identified in DoD Instruction 4650.01. Additional implementation guidance can be found in section 7.6.1 Spectrum Management Considerations.

4.4.18. Standardization

Standardization is the process of bringing products, materials, data, services, procedures, practices, and performance into conformity and consistency by means of standards. A standard establishes technical requirements for processes, procedures, practices, or methods, and can usually be classified as one of the following types: interface standards, design criteria standards, material standards, manufacturing process standards, standard practices, and test method standards.

DoD Instruction 4120.24 is the DoD policy to promote standardization of materiel, facilities, and engineering practices to improve military operational readiness, reduce total ownership costs, and reduce acquisition cycle time.

Standardization can also be used by program offices and purchasing activities as an enabling strategy to provide the warfighter with equipment that is interoperable, reliable, and technologically superior.

The use of performance-oriented interface standards generally leads to more affordable and open systems design solutions because they encourage competition and innovation while protecting intellectual property rights of suppliers. These standards also facilitate rapid insertion of new technologies and integration of parts from alternate sources and suppliers, which improves supportability and permits rapid technology refresh of military systems that are often in service for decades.

Standards define functional, physical, electronic, information, and other interface requirements needed for interoperability among the military departments and with multinational partners. Interoperability with multinational partners may require use of international standardization agreements, such as the NATO Standardization Agreements, the American-British-Canadian-Australian Armies Standardization Program, or the agreements of the Air and Space Interoperability Council.

Standardization also plays a key role in defining systems engineering best practices and processes The program manager balances the decision to use standardized agreements, practices, products, parts, processes, interfaces, and methods with required capabilities, operational environment, technology feasibility and growth, and cost effectiveness. Program managers should give preference to use of performance-based, non-government standards (NGSs) that are developed and advocated by recognized international and national standard organizations and are well accepted and supported in the commercial marketplace. NGSs are usually developed in voluntary consensus standards bodies such as the World Wide Web Consortium (W3C), the International Organization for Standardization (ISO), American National Standards Institute (ANSI), Institute of Electrical and Electronics Engineers (IEEE), and Government Electronics and Information Association (GEIA).

The DoD Information Technology Standards Registry mandates the minimum set of standards and guidelines for the acquisition of all DoD systems that produce, use, or exchange information.

The Acquisition Streamlining and Standardization Information System (ASSIST) database identifies approved defense and federal standardization documents and adopted NGSs, and is one resource program managers can use to identify standards that are applicable and appropriate for their application.

4.4.19. Supportability

4.4.19. Supportability

The program manager should address sustainment throughout the system life cycle to ensure that the system can be effectively supported (see Chapter 5 for additional information). When using an evolutionary acquisition strategy, supportability analysis activities should address performance and support requirements over the life cycle of the system for each capability increment as well as consider and mitigate any negative impact of supporting multiple system variants or variations. The supportability of the design(s) and the product support package should be cost effective and provide the necessary support to achieve peacetime and wartime readiness requirements. Supportability considerations are integral to all trade-off decisions, as directed by DoD Directive 5000.01, E1.1.29:

PMs shall consider supportability, life-cycle costs, performance, and schedule comparable in making program decisions. Planning for Operation and Support and the estimation of total ownership costs shall begin as early as possible. Supportability, a key component of performance, shall be considered throughout the system life cycle.

Supportability depends upon design features for reliability and maintainability, technical support data, and maintenance procedures to facilitate detection, isolation, and timely repair and replacement of system anomalies. (See the "Supportability Guide" for additional information.) This includes factors such as diagnostics, prognostics, real-time maintenance data collection, transportability, facility requirements, accessibility, corrosion protection and mitigation, and other factors that contribute to an optimum environment for developing and sustaining a stable, operational system with a reduced logistics footprint. The supportability posture of defense systems should be designed-in to minimize the logistics footprint since the "footprint problem" has an engineering solution.

Performance Based Logistics is the preferred product support method for DoD as directed in DoD Directive 5000.01, E1.1.17:

Performance-Based Logistics. PMs shall develop and implement performance-based logistics strategies that optimize total system availability while minimizing cost and logistics footprint. Trade-off decisions involving cost, useful service, and effectiveness shall consider corrosion prevention and mitigation. Sustainment strategies shall include the best use of public and private sector capabilities through government/industry partnering initiatives, in accordance with statutory requirements.

4.4.19.1. Supportability Analyses

The program manager conducts supportability analyses as an integral part of the systems engineering process throughout the system life cycle. The results of these analyses form the basis for the related design requirements included in the system performance specification and in the product support package documentation. The results also support subsequent decisions to achieve cost-effective support throughout the system life cycle. For systems, this includes all increments of new procurements and major modifications and upgrades, as well as reprocurement of systems, subsystems, components, spares, and services required beyond the initial production contract award. The program manager should permit broad flexibility in contractor proposals to achieve program sustainment key performance parameter and key system attributes and any associated supportability objectives.

4.4.19.2. Support Concepts

The program manager establishes logistics support concepts (e.g., organic, two-level, three-level, contractor, partnering, etc.) early in the program, and refines the concepts throughout program development. Total Ownership Cost and Materiel Availability play key roles in the overall selection process to ensure the system can be effectively supported with the minimum logistics footprint. Support concepts for all systems should be structured to provide cost effective, total life-cycle logistics support. Key Support Concept sub-elements that should be considered in developing the support concept include the following:

- Embedded Diagnostics/Testing and Prognostics,
- Embedded Training and Technical/Maintenance Data,
- Serialized Item Management supported by Automatic Identification Technology and Item Unique Identification technology,
- Reliability Centered Maintenance/Condition Based Maintenance
- Standard Data Syntax and Semantics,
- Iterative Technology Refreshment,
- Public-Private Partnerships, and
- End-to-End Supply Chain Management System.

Condition Based Maintenance Plus (CBM+) is an important support concept and a specific initiative which can be very useful in cost effectively sustaining performance. It is the application and integration of appropriate processes, technologies, and knowledge-based capabilities to improve the reliability and maintenance effectiveness of DoD systems and components. At its core, CBM+ is maintenance performed based on evidence of need provided by Reliability Centered Maintenance analysis and other enabling processes and technologies. CBM+ uses a systems engineering approach to collect data, enable analysis, and support the decision-making processes for system acquisition, sustainment, and operations. CBM+ policy is established in DoD Instruction 4151.22. Guidance of the use of CBM+ is in the "Condition Based Maintenance Plus Guidebook."

4.4.19.3. Support Data

Contract requirements for deliverable support and support-related data should be consistent with the planned support concept and represent the minimum essential requirements to cost-effectively maintain the fielded system and foster source of support competition throughout the life of the system. The program manager should coordinate government requirements for these data across program functional specialties to minimize redundant contract deliverables and inconsistencies.

4.4.19.4. Support Resources

The support resources needed, for both the total system over its expected life and for each increment of introduced capability, are inherent to 'full funding' calculations. Therefore, support resource requirements are a key element of program reviews and decision meetings. During program planning and execution, logistics support products and services are competitively sourced. See Chapter 5 for more information on establishing the support resources to be included in the product support package. The following are examples of things the program manager can consider in the design process that can increase the materiel availability, lower the life-cycle cost, and reduce the logistics footprint:

- Embed training and maintenance techniques to enhance user capability and reduce life-cycle costs, and
- Base automatic test system (ATS) selection on a cost and benefit analysis over the complete system life cycle. Minimize the introduction of unique types of ATS into the DoD field, depot, and manufacturing operations by using standard ATS families or Commercial-off-the-shelf components that meet ATS capability needs for test hardware and software. Also, consider the mix of diagnostic, prognostic, system health management, and automatic identification technologies in the ATS trade-off process.

4.4.20. Survivability and Susceptibility

The program manager should fully assess system and crew survivability against all anticipated threats at all levels of conflict early in the program, but in no case later than entering System Demonstration and Demonstration. This assessment also considers fratricide and detection. If the system or program has been designated by the Director, Operational Test and Evaluation (DOT&E), for Live Fire Test and Evaluation (LFT&E) oversight, the program manager should integrate the test and evaluation (T&E) used to address crew survivability issues into the LFT&E program supporting the Secretary of Defense LFT&E Report to Congress.

In accordance with DoD Instruction 3150.09, The Chemical, Biological, Radiological, and Nuclear (CBRN) Survivability Policy, the program manager should address (CBRN) survivability for all mission critical systems whose operating environment would include operating in a CBRN environment according to the Systems Threat Assessment Report (STAR)

or in lieu of a STAR the appropriate Capstone Threat Document. Cost-effective survivability techniques and a plan for the validation and confirmation of CBRN survivability should be developed. It should be noted that High Altitude Electromagnetic Pulse (HEMP) is the main concern of the Nuclear portion of CBRN for those mission critical systems containing electronics.

The program manager should establish and maintain a survivability program throughout the system life cycle to attain overall program objectives. The program should stress early investment to provide a balanced survivability approach that enables the platform to satisfy mission effectiveness and operational readiness requirements by:

- Incorporating susceptibility reduction features that prevent or reduce engagement of threat weapons including but not limited to those in the radar, infrared, acoustic and visual spectrums. These features should balance use of signature reduction with countermeasures employment to attain overall program mission requirements,
- Providing mission planning and dynamic situational awareness features to enable tactical threat avoidance capabilities
- Incorporating vulnerability reduction features including damage tolerance in system design. These features should balance the use of a robust structural design including hardening and redundancy of critical components, fire prevention/ detection/suppression and software reconfiguration to enable continued use of critical systems under degraded conditions.
- Providing casualty reduction design features to reduce personnel casualties resulting from damage to or loss of the aircraft;
- Maximizing wartime availability and sortie rates via threat damage tolerance and rapid reconstitution(reparability) features compatible with the environment the platform is based from; and
- Balancing overall survivability requirements with other design characteristics and program cost, schedule and performance requirements.

Unless waived by the Milestone Decision Authority, mission-critical systems, including crew, regardless of acquisition category, should be survivable to the threat levels anticipated in their projected operating environment as portrayed in their platform specific System Threat Assessment Report (STAR) or in lieu of a STAR the appropriate Capstone Threat Document. Design and testing ensure that the system and crew can withstand man-made hostile environments without the crew suffering acute chronic illness, disability, or death.

4.4.21. Unique Identification of Items

Item Unique Identification (IUID) is a systematic process to globally and unambiguously distinguishing one item from all other items that the DoD buys or owns, allowing the DoD to track and manage identically made items individually throughout their life cycles. With IUID, DoD can consistently capture the value of all individual items it buys, trace these items during their use, combat counterfeiting of parts, and associate valuable business intelligence to an item

throughout its life cycle via automatic identification technology and connections to automated information systems.

IUID policy requires that qualifying DoD items, as specified in Defense Federal Acquisition Regulation Supplement (DFARS) 211.274-2, are marked with a two-dimensional data matrix that is encoded with a Unique Item Identifier (UII). The UII consists of the manufacturer's Commercial and Government Entity (CAGE) Code, and unique serial number at a minimum and may also contain original part number if desired. The unique identifier is permanent and is assigned to the individual item for its entire life; regardless of changes to its configuration or part number. The UII is a universal key that allows linkages to other systems and processes to provide asset visibility (item identification, custodian, condition) allowing DoD to consistently locate, control, value, and manage its assets. The mark is also useful to link the item to other sustainment processes, event history databases, and production management systems for repairable items. UIIs are registered in the DoD IUID Registry, along with pedigree data associated with the item.

Systems Engineering efforts to support IUID implementation can be found in chapter 2 of the DoD Guidelines for Engineering, Manufacturing and Maintenance Documentation Requirements for Item Unique Identification (IUID) Implementation.

The following sources provide useful information about IUID:

- IUID policy announcements,
    - DoD Directive 8320.03, "Unique Identification (UID) Standards for a Net-Centric Department of Defense," March 23, 2007,
    - DoD Instruction 8320.04, "Item Unique Identification (IUID) Standards for Tangible Personal Property," June 16, 2008,
    - DoD Instruction 5000.64, "Accountability and Management of DoD-Owned Equipment and Other Accountable Property," November 2, 2006, and
    - DoD Instruction 4151.19, "Serialized Item Management (SIM) for Materiel Maintenance," December 26, 2006.
- DoD guides for IUID implementation and planning,
- DFARS 211.274, "Unique Item Identification and Evaluation,"
- MIL-STD-130, "Identification Marking of U.S. Military Property,"
- MILS-STD-129, "Military Marking for Shipment and Storage,"
- Information on the DoD IUID Registry procedures, and
- Information on IUID training, and
- Systems Engineering Plan Preparation Guide for Annex A.

4.5. Systems Engineering Execution: Key Systems Engineering Tools and Techniques

This section describes some of the systems engineering techniques and tools for management, oversight, and analysis and provides some general knowledge management resources.

4.5.1. Systems Engineering Plan (SEP)

The purpose of the SEP is to help program managers develop their systems engineering approach, providing a well thought out and documented technical foundation for the program. The SEP is a living document in which periodic updates capture the program's current status and evolving systems engineering implementation and its relationship with the overall program management effort. The SEP is a detailed formulation of actions that should guide all technical aspects of an acquisition program. Program managers should establish the SEP early in program formulation and a best practice is to have the SEP written by the program Systems Engineering Working-level Integration Team. Formal SEP updates signed by the Milestone Decision Authority are required for acquisition milestone decisions, program restructures, and/or program deviations. Informal SEP updates should be approved by the lead/chief systems engineer and program manager before each technical review. It is a roadmap that supports program management by defining comprehensive systems engineering activities, addressing both government and contractor technical activities and responsibilities. The SEP should be consistent with and complementary to the Acquisition Strategy and the Test and Evaluation Strategy or Test and Evaluation Master Plan, as appropriate. This chapter of the Defense Acquisition Guidebook, in conjunction with the SEP Preparation Guide and SEP Frequently Asked Questions, should be used as guidance when preparing a SEP.

The SEP describes the program's overall technical approach, including systems engineering processes; resources; and key technical tasks, activities, and events along with their metrics and success criteria. Integration or linkage with other program management control efforts, such as Integrated Master Plans, Integrated Master Schedules, Technical Performance Measures, risk management, and Earned Value Management, is fundamental to successful program execution.

There is no prescribed format for the SEP; however, it should address how systems engineering will support the translation of system capability needs into an effective, suitable product that is sustainable at an affordable cost. Specifically, a well-prepared SEP will address the integration of the technical aspects of the program with the overall program planning, systems engineering activities, and execution tracking to include the following:

- **The overall requirements for the program.** These include the Initial Capabilities Document-/Capability Development Document-/Capability Production Document-derived key performance parameters-/key system attributes, statutory and regulatory requirements, certification requirements, derived requirements, and design constraints. Most importantly, the SEP should address how the program will capture, integrate, and manage all of these differing types of requirements as an integrated whole, so as to ensure that the requirements are traceable to the design, verification, and validation of the system. It should also describe how the program will ensure transparency of these requirements to various stakeholders throughout development.
- **The systems engineering processes to be applied in the program** (e.g., from a standard, a capability maturity model, or the contractor's process). These include a description of how the processes will be implemented and how they will be tailored to

meet individual acquisition phase objectives. Also included is an explanation of how the systems engineering processes will support the technical and programmatic products required of each phase. Section 4.2 (process) and section 4.3 (process application by systems engineering phase) provide a "roadmap" of how systems engineering processes can be applied to an acquisition program throughout the system life cycle.

- **The integration of systems engineering into the program's integrated product teams (IPTs).** This describes how systems engineering activities will be integrated within and coordinated across IPTs; how the IPTs will be organized; what systems engineering tools they will employ; and their resources, staffing, management metrics, and integration mechanisms. It also explains how systems engineering activities are integrated in the program's overall integrated master plan and schedule (section 4.5.2 and section 4.5.3).
- **The system's technical baseline approach.** This includes a description of how the technical baseline will be developed, managed, and used to control system requirements, design integration, verification, and validation. It includes a discussion of metrics (e.g., Technical Performance Measures) for the technical effort and how these metrics will be used to measure progress.
- **Event-driven timing, conduct, success criteria, and expected products of technical reviews**, and how technical reviews will be used to assess technical maturity, assess technical risk, and support program decisions. SEP updates will include results of completed technical reviews. Section 4.3 of this guide, as well as other reference material on technical reviews, should form a basis for the program's approach.
- For programs that are part of a system of systems or family of systems, **the synchronization with related systems** to achieve the desired mission capability as the system evolves. The relative contribution of each system to the overall mission capability in terms of performance and effectiveness should be identified to ensure that the combination of systems is appropriately integrated together.
- Incorporate HSI Planning into the SEP.

In addition to describing required program activities, the SEP addresses the, who, what, when, where, why, and how of the systems engineering approach.

- **Participants in the Systems Engineering Process (Who)**—Ideally, the SEP should detail roles and responsibilities of the systems engineering efforts across the government and contractor boundaries. Roles of the chief engineer, lead systems engineer, IPT systems engineers, Systems Engineering Working-level Integration Team, etc., need to be explicitly defined. Vertical and horizontal integration, team communications, and scope of decision-making authority are key elements of the plan, especially as these relate to management of technical baselines and reviews. Systems engineering staffing (planned vs. actual) should be included in this discussion together with (required vs. actual) discussion of domain experience of the staff.
- **Systems Engineering Processes and Products (What)**—There are numerous approaches to accomplish systems engineering and it is critical to the plan how the program selects and implements the best approach. There is a difference between complexity and uncertainty. While systems engineering is complex, it should not be

uncertain. The SEP should serve as a vehicle for minimizing process uncertainty. Optimally, a program team should use a single set of common systems engineering processes. For large programs having multiple organizations, this may be an impractical goal. In these cases, the program manager should strive to "rationalize" or link the different process implementations across the program team so that process inputs and outputs integrate. The SEP should also detail how the products of the systems engineering approach, namely the functional, allocated, and product baselines, will be developed and managed. These baselines should include both design requirements and verification/validation requirements for all configuration items across the Work Breakdown Structure. Relationship of the baselines to the planned specification tree should be described.

- **Facilities Enabling Systems Engineering (Where)**—The SEP should address development and use of systems engineering facilities/laboratories, including verification and validation facilities. Since these facilities can be complex hardware and software systems in their own right, the issue of integration facilities can be a significant challenge. Integration is particularly complex as it relates to development of modeling and simulation requirements and the resources (time and funding) needed to establish (develop, modify, or adapt) the required facilities/laboratories.
- **Systems Engineering Event Timing (When)**—Systems engineering is an event-driven process based on successful completion of key events vice arbitrary calendar dates. As such, the SEP should discuss the timing of events in relation to other systems engineering and program events. While the initial SEP and Integrated Master Schedule will have the expected occurrence in the time of various milestones (such as overall system CDR), the plan should accommodate and be updated to reflect changes to the actual timing of systems engineering activities, reviews, and decisions.
- **Systems Engineering Decision Rationale (Why)**— Systems Engineering includes a continuous evolution of requirements (from high-end to detail-level) and trade-offs (to best balance the design across often-conflicting design considerations). Rationale as to how these requirements and trades will be balanced should be included in the SEP. Decision criteria, such as entry and exit criteria for technical reviews, should be detailed.
- **Tools Enabling Systems Engineering (How)**—Systems engineering makes use of a number of tools, toolsets, and enablers, such as modeling and simulation. The capability, variety, and dynamics of modern systems engineering tools demand that they be fully integrated with the overall approach and discussion of systems engineering application. Since adaptation of tools often occurs on programs, continual update of the SEP is required.

For programs where the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) or the Assistant Secretary of Defense for Networks and Information Integration is the Milestone Decision Authority (MDA), the appropriate Component Acquisition Executive should submit the final SEP to the office of the Director, Systems Engineering, Deputy Director for Major Program Support (SE/MPS) (or designated representative) for Director of Systems Engineering (Dir, SE) approval no later than 30 days before the milestone decision. Best practice is to submit the SEP no later than 30 days before the anticipated approval date of the Acquisition

Strategy, so that the SEP can support major acquisition actions such as release of any requests for proposals. The Dir, SE is the approval authority for the SEP (see Directive-Type Memorandum (DTM) 09-027 – Implementation of the Weapon Systems Acquisition Reform Act of 2009). Upon adjudication of SEP comments, SE/MPS will forward the SEP to the Dir, SE for approval.

4.5.2. Integrated Master Plan (IMP)

The program manager should use event-driven schedules and the participation of all stakeholders to ensure that all tasks are planned and accomplished in a rational and logical order and to allow continuous communication. Necessary entry criteria to initiate each major task should be identified, and no major task should be declared complete until all required exit criteria have been satisfied. When documented in a formal plan and used to manage the overall program, this event-driven approach can help ensure that all tasks are integrated properly and that the management process is based on the accomplishment of significant events in the acquisition life cycle and not on arbitrary calendar dates.

One way of defining tasks and activities is the use of an Integrated Master Plan (IMP), which provides an overarching framework against which all work is accomplished. It documents all the tasks required to deliver a high quality product and facilitate success throughout the product's life cycle. Cost, schedule (specific dates), and non-essential tasks are not included in this plan. During the initial stages of a program, the integrated plan is preliminary, and its purpose is to provide an understanding of the scope of work required and the likely structure of the program. It is constructed to depict a likely progression of work through the remaining phases, with the most emphasis on the current or upcoming phase (especially the period to be contracted for next). The integrated plan also serves to identify dependencies, which may be performed by different organizations.

As the program is defined, the IMP is iterated several times, each time increasing the level of detail and confidence that all essential work has been identified. The specific format for this plan is not critical; however, it usually reflects an Event/Accomplishment/Criteria hierarchical structure, a format that greatly facilitates the tracking and execution of the program. Functional and life-cycle inputs are required to integrate the processes and products of the program. Without formal documentation such as an Integrated Master Plan, these inputs may be lost when personnel change. Such a plan also defines and establishes the projected expectations.

Deriving the program schedule presents an opportunity to identify critical risk areas. As the times to complete specific tasks are estimated, events that may cause delays will become apparent. These events are potential areas of risk that the program manager should consider for further analysis and possible mitigation.

4.5.3. Integrated Master Schedule (IMS)

Executable planning and schedules need to be built first with a fundamental understanding of the technical products required and then the time necessary to develop these products. For an Integrated Master Schedule (IMS) to be effective a work breakdown structure (WBS) should first be developed based on the overall system's physical architecture (system building blocks) identifying all of the major systems and subsystems down to a configuration item level. Once this is completed, the activities required to define, design, integrate, test, evaluate and deliver the system elements should be defined. These activities can then be further defined in terms of calendar time and resources to complete. Following this definition, they can be assembled into an integrated, event-based, and resource-based schedule. One way to produce such a schedule is to develop an IMS based on an Integrated Master Plan (IMP) and a fully detailed WBS (see IMP/IMS Guide, page 34 and Figure 4.5.3.F1).

With an IMP, the IMS further helps the program manager understand the links and interrelationships among the various activities and people performing them. At a minimum, an IMS shows the expected start and stop dates for each task in the plan, but each task may be broken down into lower-level tasks that will be used to manage the program on a day-to-day basis. The schedule can be expanded downward to the level of detail appropriate for the scope and risk of the program. Programs with high risk show much lower levels of detail in the IMS to give the visibility to manage and control risk. The more detailed the IMS, however, the greater the cost to track and update the schedule. The dates in the IMS should not be made contractually binding to allow the flexibility to take full advantage of event-driven scheduling.

Each of the work products requires different levels of effort, personnel, resources, and time to complete, with some being more difficult to complete than others. Critical Path Analysis is used to help identify which tasks, or sets of tasks, will be more difficult or costly to complete. As many of the tasks are interrelated and as work products typically require the completion of all lower level tasks before the higher-level work product can be completed, the early identification of critical tasks is essential for ensuring that schedule and cost goals are maintained for the program.

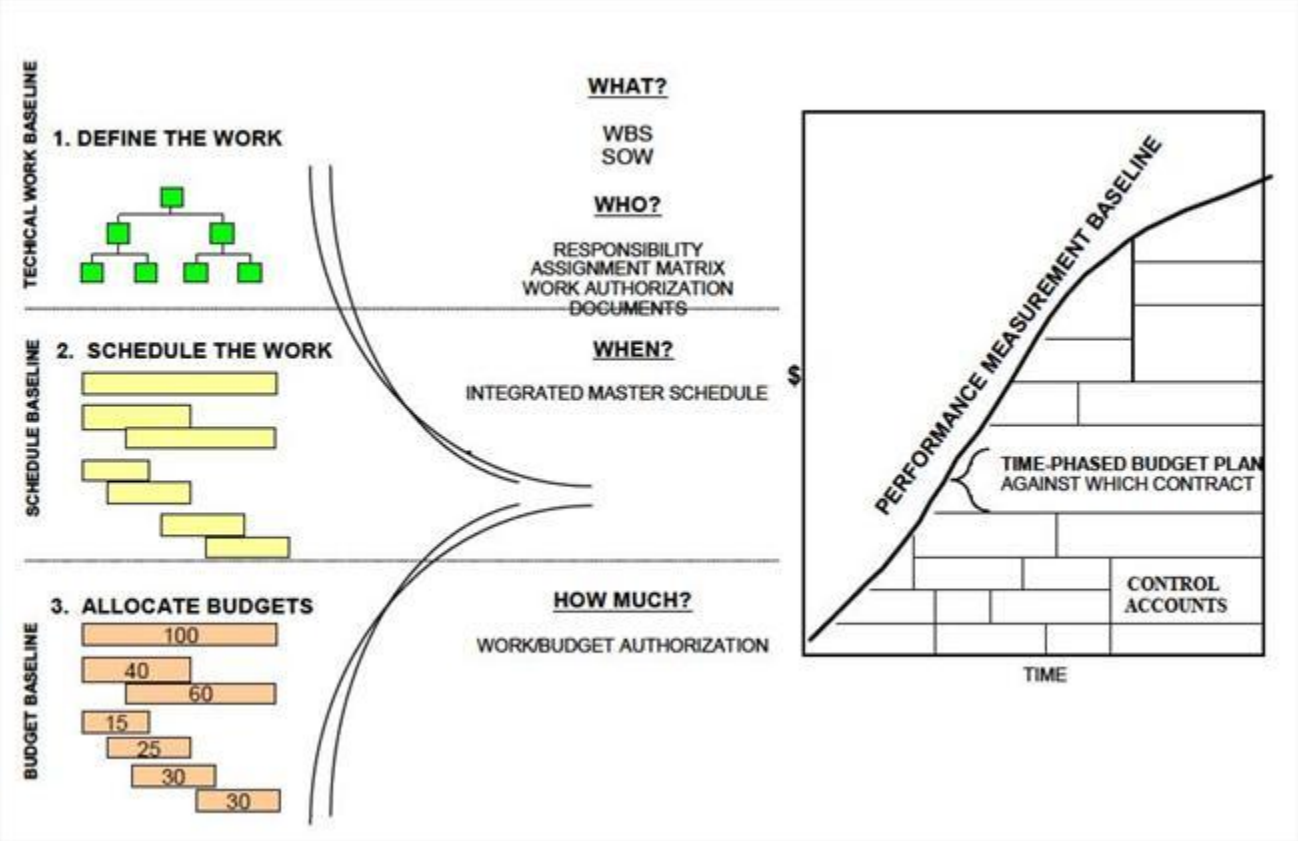


Figure 4.5.3.F1. Developing an Integrated Master Schedule

4.5.4. Earned Value Management (EVM) and Work Breakdown Structure (WBS)

4.5.4.1. Earned Value Management (EVM)

EVM is an important tool used by Program Managers and Systems Engineers in the Technical Assessment Process to appraise the program technical progress against the Performance Measurement Baseline (PMB). The mandated requirement to implement EVM on all Acquisition Category I programs is presented in Section 11.3.1. Systems Engineering is responsible for characterizing the entire technical scope of effort in the Work Breakdown Structure (WBS) and the corresponding event driven program implementation in the Integrated Master Schedule (IMS). The WBS and IMS form the basis of the PMB and the foundation of EVM. (See also the Program Managers' Guide to the Integrated Baseline Review Process, page 6.)

4.5.4.2. Work Breakdown Structure (WBS)

A WBS is a product oriented family tree composed of hardware, software, services, data and facilities that completely define a program. Systems engineering is critical in the identification of product elements of the WBS. The WBS displays and defines the product(s) to be developed and/or produced and relates elements of work to be accomplished to the end product.

The WBS is defined, developed, and maintained throughout the system life cycle based on disciplined application of the systems engineering process.

A WBS can be expressed to any level of detail. However, the top three levels are the minimum recommended for reporting purposes unless the items identified are high cost or high risk. Then, and only then, is it critical to define the product at a lower level of WBS detail.

The WBS is the foundation for:

- Program and technical planning,
- Cost estimation and budget formulation,
- Schedule estimation,
- Statements of work and specification of contract line items, and
- Progress status reporting and problem analysis.

MIL-HDBK-881A, Work Breakdown Structures for Defense Materiel Items, should be used as the basis for developing a WBS.

Technical Performance, Integrated Cost, Schedule and Risk Management – Planning tasks by WBS elements serves the basis for mapping the development of the technical baseline for estimating and scheduling resource requirements (people, facilities and equipment) and mitigating risks. By breaking the total product into successively smaller entities, program managers can ensure all required products are identified in terms of technical performance, cost, and schedule and goals in order to reduce risk.

Performance measurement of WBS elements, using objective measures, is essential for Earned Value Management and Technical Assessment activities to determine program progress. These objective measures are used to report progress in achieving milestones and should be integrated with Technical Performance Measures and Critical Technical Parameters.

The systems engineering process ensures that as the lower levels of the product elements of the WBS are developed and they continue to satisfy the operational needs specified in the Capability Development Document and allocated to the system specification. The systems engineering process also ensures that any changes to the portions of the WBS under contractor control are conducted using trade-off processes and criteria that maintain system integrity.

4.5.5. Value Engineering (VE)

4.5.5. Value Engineering (VE)

The requirement for the DoD VE program is codified in 41 U.S.C. 432. The program is intended to reduce costs, increase quality, and improve mission capabilities across the entire spectrum of DoD systems, processes, and organizations. It employs a simple, flexible, and structured set of tools, techniques, and procedures that challenge the status quo by promoting innovation and creativity. Furthermore, it incentivizes government participants and their industry counterparts to increase their joint value proposition in achieving best value solutions as part of a successful business relationship. Where appropriate, program managers should engage in a broad and rigorous application of the VE methodology.

In addition, program managers should be receptive to Value Engineering Change Proposals (VECPs) made by contractors as a way of sharing cost savings and should also ensure that implementation decisions are made promptly. A VECP is a proposal submitted by a contractor under the VE provisions of the Federal Acquisition Regulation that, through a change in the contract, would lower the project's life-cycle cost to DoD. This contract change requirement can be the addition of the VECP to the contract, with attendant savings. VECPs are applicable to all contract types, including performance based contracts.

A common misconception is that VE applies only to production. The most opportune time to apply the VE methodology is early in the life cycle, before production begins, before field or technical manuals are drafted, and before logistic support plans are finalized. Some of the more important benefits are as follows:

- Savings can be applied to all production units,
- Reductions to the high cost of development, the subsequent cost of production, and the consequent costs related to operation and support may be realized,
- Fewer modifications to production lines, tooling, processes, and procedures will be required,
- Fewer drawing changes will be necessary, and
- Fewer post-production changes to logistic and support elements such as manuals, maintenance facilities, and spare parts requirements will be needed.

Also, in today's acquisition environment, many systems remain in inventory for a long time because of major modifications or upgrades (e.g., block changes or preplanned product improvements). Therefore, opportunities for large VE savings begin in early program phases and extend late into sustainment.

Additional VE resources are available as a Defense Acquisition University (DAU) Continuous Learning Module (click on CLE001) and on the Institute for Defense Analyses website and the DAU website.

4.5.5.1. Value Engineering (VE) in Materiel Solution Analysis

VE can have a significant role in the systems engineering activities during Materiel Solution Analysis. The analysis of alternatives and associated cost-effectiveness studies can use VE to analytically evaluate functions and provide a mechanism to analyze the essential requirements and develop possible alternatives offering improved value.

4.5.5.2. Value Engineering (VE) in Technology Development

In support of the process to transition technology from the technology base into program-specific, preliminary, design efforts, VE can be used to analyze the value of each requirement and the specifications derived from it by comparing function, cost, and worth.

4.5.5.3. Value Engineering (VE) in Engineering and Manufacturing Development

As part of the development and refinement of the functional baseline, VE should be used for: 1) identifying the necessary top-level functions for each of the missions considered, 2) identifying technical approaches (i.e., design concept) to the missions, 3) identifying necessary lower level functions for each technical approach (the value engineer should place emphasis on eliminating unnecessary design restrictive requirements), 4) evaluating each function in terms of technical feasibility, and 5) estimating the cost of various functions.

4.5.5.4. Value Engineering (VE) in Production and Deployment

VE contributes to the systems engineering activities during production and deployment by devising alternative means for achieving required functions and developing alternative designs to meet functional needs. VE has been extensively applied to evaluate and improve manufacturing processes, methods, and materials.

4.5.5.5. Value Engineering (VE) in Operations and Support

After fielding, opportunities for VE may exist for a long time. Product life cycles are being extended; for consumables, there is no sure way to determine the total quantity that will be purchased. Also, in the past, many items that entered the defense inventory were never subjected to a VE analysis. The potential for VE savings on these items is real. Advances in technology or changes in user requirements provide a basis for potential savings.

4.5.6. Types of Technical Assessments

4.5.6.1. Technical Performance Measurements (TPMs) and Critical Technical Parameters (CTPs)

TPMs and CTPs compare the actual versus planned technical development and design. They report progress in the degree to which system performance requirements are met. Systems engineering uses TPMs and CTPs to balance cost, schedule, and performance throughout the life cycle when integrated with other management methods such as the work breakdown structure (WBS) and Earned Value Management System. CTPs are TPMs used to track the performance measurement of metrics used is support of test and evaluation.

At the start of a program, TPMs define the planned progress of selected technical parameters. The plan is defined in terms of expected performance at specific points in the program as defined in the WBS and Integrated Master Schedule, the methods of measurement at those points, and the variation limits for corrective action. During the program, TPMs record the actual performance observed of the selected parameters and assist the manager in decision-making (performance or resource tradeoffs) through comparison of actual vs. projected performance. TPM parameters that especially need to be tracked are the cost drivers on the program, those that lie on the critical path, and those that represent high technical risk items.

A well thought out program of TPMs provides an early warning of technical problems and supports assessments, and provides an assessment of the impacts of proposed changes in system performance. To accomplish this, the government and contractor both need to set parameters to be tracked.

The government program office will need a set of TPMs that provide visibility into the technical performance of key elements of the work breakdown structure and the highest areas of cost, schedule, or technical risk. The TPMs selected for delivery to the government are expected to be traceable to the needs of the operational user and to the set of key performance parameters, key system attributes, and CTPs.

The contractor will generally track more items than are reported to the government, as the contractor needs information at a more detailed level than does the government program office. TPM reporting to the government is a contractual issue, and those TPMs on which the government receives reports are defined as contract deliverables in the contract data requirements list.

4.5.6.2. Program Support Review (PSR)

The PSR is conducted to provide insight into current and future program execution through detailed analysis using the "Defense Acquisition Program Support Methodology." OSD system assessment teams apply the Defense Acquisition Program Support (DAPS) methodology to Major Defense Acquisition Programs (MDAPs) approaching a Defense Acquisition Board (DAB) review. DAPS, however, is also a powerful self-assessment tool for the program manager to use for technical evaluation of a program's systems engineering process details and health.

DoD Instruction 5000.02, Enclosure 2, paragraph 9.f, directs the following:

PSRs shall be conducted by cross-functional and cross-organizational teams appropriate to the program and situation. PSRs for ACAT ID and IAM programs shall be planned by the Director, Systems and Software Engineering [effective 22 May 2009, the Director, Systems Engineering (SE)] to support OIPT program reviews, at other times as directed by the USD(AT&L), and in response to requests from PMs.

The DAPS methodology addresses the systems engineering policies set forth by the Defense Acquisition Executive. These policies foster effective systems engineering practices on all programs, helping the program manager attain success in the acquisition and support life cycle. The thorough application of the DAPS methodology can contribute to improved balance of cost, schedule, performance, and risk.

The "Defense Acquisition Program Support Methodology" is a guidebook for conducting PSRs that will assist program managers prepare for Milestone A, B, and C decision reviews. It contains a listing of programmatic and technical areas, sub-areas, and factors, developed to be both broad in scope, as well as specific (detailed) enough to enable application to programs of all types. The DAPS methodology was constructed from numerous documents in the Defense acquisition community, and exploits the expert knowledge of "greybeard" human resources with years of acquisition experience in both government and industry. Sources include the Software Engineering Institute's Capability Maturity Model and Capability Maturity Model Integration, NAVAIR Systems Engineering Technical Resources Handbook, Air Force assessment guidance, Manufacturing Best Practices/Willoughby Templates, OSD Acquisition guidelines and policies, and many subject matter experts from across the DoD community.

The PSR team will use the DAPS methodology in preparation for structuring the scope and focus of review areas of interest. During the reviews, through interviews and discussions, the PSR teams perform the following tasks:

- Identify program strengths, problems, risks and other issues,
- Categorize and relate the defined findings (triggering vs. symptomatic),
- Prioritize these findings with respect to program impact, and
- Develop actionable recommendations that address final program findings (focus on root causes.

The team analyzes their PSR findings and briefs and adjudicates the documented results to and with the program managers and prime contractors. The completed report is then forwarded to OSD management to assist with program acquisition decisions.

The results of the PSR are intended to provide:

- Actionable recommendations to Program Management Offices to facilitate successful execution of their programs,
- Support to Under Secretary of Defense for Acquisition, Technology and Logistics decision-making process for MDAP and Major Automated Information System programs, and
- A means to conduct a systemic analysis of programs to identify opportunities to improve acquisition performance through changes in policy, education, and effective use of systems engineering.

The Director of Systems Engineering shall have access to any DoD component records or data relating to systems engineering and development planning (including classified, unclassified, competition sensitive, and proprietary information) necessary to carry out assigned duties (see Directive-Type Memorandum (DTM) 09-027 – Implementation of the Weapon Systems Acquisition Reform Act of 2009).

4.5.6.3. Assessment of Operational Test Readiness (AOTR)

The AOTR is conducted to provide insight into the readiness of a program to proceed with current and future program execution through detailed analysis using the "Defense Acquisition Program Support Methodology."

DoD Instruction 5000.02, Enclosure 6, paragraphs 4.b and 4.c, direct the following:

The DUSD(A&T) shall conduct an independent Assessment of Operational Test Readiness (AOTR) for all ACAT ID and special interest programs designated by the USD(AT&L). Each AOTR shall consider the risks associated with the system's ability to meet operational suitability and effectiveness goals. This assessment shall be based on capabilities demonstrated in DT&E and OAs and criteria described in the TEMP. Where feasible, the AOTR shall be performed in conjunction with the program's review and reporting activities as described in...The AOTR report shall be provided to the USD(AT&L), DOT&E, and CAE.

The CAE shall consider the results of the AOTR prior to making a determination of materiel system readiness for IOT&E.

4.5.7. Trade Studies

Trade studies are used in support of decision making throughout the life cycle of a program. Trade studies are conducted among operational capabilities, functional, and performance requirements, design alternatives and their related manufacturing, testing, and support processes; program schedule; and life-cycle cost to systematically examine alternatives. Once alternatives have been identified, a trade study team applies a set of decision criteria to analyze the alternatives. These criteria are 'traded' to determine which alternative is optimal and to be recommended.

Most trade studies are not strictly formal or informal; usually they fall somewhere in between these two extremes. As a general rule, formal trade studies are indicated for high-value, high-risk or other high-impact decisions. Not all trade studies should follow the full rigor of a formal process, but should be tailored to the specific circumstances of the program such as:

- Likelihood or severity of programmatic risk,
- Objectivity and quantitative data used,
- Detail in available data, and
- Time, effort and money needed to conduct the trade study.

Additional information on conducting trade studies is available in a Defense Acquisition University (DAU) Continuous Learning Module CLE 026, "The Preferred Practices Approach to Trade Studies".

4.5.8. Modeling and Simulation (M&S)

M&S capabilities and limitations are often inadequately understood, and M&S is sometimes not planned and/or managed with sufficient care. Although we can credibly model many things we understand well (e.g., physical capabilities, natural phenomena, and physics-based interactions), it is much more difficult to reliably represent things we do not understand well (e.g., human behavior, reliability, and emergent behaviors of complex systems). M&S capability involves not just the software tools themselves, but the data that feeds them; the computing platforms that execute them; the standards, middleware and networks that may interconnect them; the encryption capabilities and security constraints that protect them; and, most importantly, the people that plan, develop, integrate, verify, validate, accredit and use them. Deficiencies in any of these present a risk to a program. Thus acquisition managers should approach the use of M&S wisely and plan carefully.

The following links provide policy and guidance for modeling and simulation:

- DoD Directive 5000.59 "DoD Modeling and Simulation (M&S) Management"
- DoD Instruction 5000.61 "DoD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A)"
- DoD 5000.59-M "DoD Modeling and Simulation (M&S) Glossary
- Recommended Practices Guide for VV&A
- Modeling and Simulation Guidance For The Acquisition Workforce

4.5.9. Summary of Technical Reviews

Technical reviews are an important oversight tool that the program manager can use to review and evaluate the state of the system and the program, re-directing activity if necessary. Figure 4.3.F1 shows the relative timing of each of the technical reviews, technically oriented program reviews, and technology readiness assessments. The commonly used reviews during most acquisition programs are the following:

- Initial Technical Review
- Alternative Systems Review
- System Requirements Review
- Technology Readiness Assessment
- Integrated Baseline Review
- System Functional Review
- Preliminary Design Review
- Critical Design Review
- Test Readiness Review
- Flight Readiness Review
- System Verification Review
- Functional Configuration Audit
- Production Readiness Review
- Operational Test Readiness Review
- Physical Configuration Audit
- In-Service Review

To learn more about the role of technical reviews in technical management throughout the program's life cycle, consider taking the Technical Reviews continuous learning module, CLE003, offered by the Defense Acquisition University.

To assist in the preparation for, and conduct of technical reviews, technical review risk assessment checklists are available for each of the reviews. These checklists are designed as a technical review preparation tool, and should be used as the primary guide for the risk assessment during the review. The checklist itself can be both an input to, and an output of, the review. The Integrated Product Team can do a self-assessment as input, but the review participants should take ownership of the assessed risk as an output of the review. These checklists are available on the Systems Engineering Community of Practice.

NOTE: The technical reviews listed above and described in Section 4.3 are detailed reviews conducted between the program management office and contractor personnel to assist the program manager and contractor in assessing technical progress of the program. Unlike these technical reviews, the Full-Rate Production Decision Review is a Milestone Decision Authority-led management oversight review intended to provide an assessment (cost, schedule, and performance) of a program's readiness to enter Full-Rate Production.

4.6. General Knowledge Tools

4.6. General Knowledge Tools

Section 804 of the National Defense Authorization Act of 2003, "Improvement of Software Acquisition Processes," requires the Assistant Secretary of Defense for Networks and Information Integration and the Under Secretary of Defense for Acquisition, Technology and Logistics to assist the secretaries of the military departments and the heads of the Defense Agencies to carry out software acquisition improvement programs. Specifically, Section 804 included a requirement for establishing a clearinghouse for information regarding best practices in software development and acquisition in both public and private sectors. Integral to establishing a clearinghouse is the need to capture and vet practice implementation experience or best practices from the workforce. To date, project/program case studies and lessons learned are the primary input for capturing practice experience.

In compliance with the Section 804 legislation, and to support the broader scope of systems engineering revitalization, the DoD Acquisition Best Practices Clearinghouse (BPCh) was established to become the central DoD clearinghouse for system acquisition best practices, including program management, development and sustainment system acquisition practices. In the future, the BPCh will continue to provide critical evidence for decision-making support as practitioners implement system, software and acquisition programs/projects within DoD. Sources of such evidence include:

- Experience reports describing the results of using specific practices;
- Case studies, which analyze a given program in some detail along with the practice(s) applied;
- Lessons learned which provide specific and focused information on a particular practice or type of project.

4.6.1. Best Practices

Best Practices represent effective strategies, gained by experience in practice, for making programs successful, whether for developing a system or for making the right choice in acquiring system components. If the right Best Practices are applied, they help to avoid common problems and improve quality, cost, or both. However, finding and selecting an appropriate best practice is not always an easy endeavor. While there are practices, including those described in this Guidebook that should be considered for every project, a single practice can never be a 'silver bullet' for each and every project/program. Some practices may only be useful or beneficial in certain contexts while failing to produce the desired results in others. For example, practices that are absolutely necessary for large, mission critical projects may not be practical for rapid prototyping or small web application development projects. Practices that work well when the development team is co-located may not always work well when the team is distributed across the country. Clearly, there exists no one best answer; practices that are best for one user might not be best for the next!

To reflect these issues, the concept of a 'practice' as defined in the DoD Acquisition Best Practices Clearinghouse (BPCh) includes:

- A description of what the practice is (e.g. what process should be followed);
- A list of resources that support the application of the practice (e.g. templates, forms, publications);
- A list of the available evidence regarding that practice (i.e. where it has been applied, what type of program it was applied on, and what the results were);
- The ability for the acquisition workforce to comment on the existing knowledge about the practice and to share their experiences, which may corroborate or contradict what is already known.

In this way, the BPCh can provide more than just a list of best practices. It is a web-based portal that includes an integrated set of processes, tools, and resources which will enable information seekers to identify emerging or well-proven practices that have been implemented and proven effective. Practices in the BPCh serve as an information resource to individuals looking for ideas on how to improve quality and become more effective in their job. For example, BPCh responds to user queries with a list of practices rated by how well they fit the project characteristics of the user making the query.

The BPCh, along with several other DoD workforce knowledge sharing systems (i.e., the Acquisition Knowledge Sharing System, the Acquisition Community Connection and ACQuire search system), will play an integral part in Defense Acquisition University's Acquisition Knowledge Management System (AKMS).

Additional best practices links include:

- The DoD Acquisition Best Practices Clearinghouse (BPCh);
- The Government Accountability Office:

    - Stronger Management Practices Are Needed to Improve DOD's Software-Intensive Weapon Acquisitions
    - Better Matching of Needs and Resources Will Lead to Better Weapon System Outcomes; and
- The Systems Engineering Community of Practice

4.6.2. Case Studies

Case studies are in-depth explorations of what happened on a particular program. Personnel from programs that are similar to the subject of the case study can especially benefit from reading what went right or wrong in a similar environment.

- The Office of the Under Secretary of Defense (Acquisition, Technology, and Logistics), Office of Systems Engineering, has published several Integrated Product and Process Development case studies
- The Air Force Center for Systems Engineering (Case Studies) has several case studies available.

4.6.3. Lessons Learned

Lessons learned are a tool that the program manager may use to help identify potential areas of risk associated with the system by reviewing the experiences encountered in past programs. Lessons learned databases document what worked and what did not work in past programs, in the hopes that future programs can avoid the same pitfalls. Lessons learned can be found at all levels of the program: managerial, system, sub-system, and component.

Lessons learned are most effective when analogous programs and systems are identified, and the lessons learned are applied with discretion and proper judgment, as opposed to non-applicable lessons being blindly followed.

Ideally, a program manager searches lessons learned databases for analogous systems, enabling the program manager to be better prepared to defuse potential problems before they become real problems or to see what solutions to similar problems worked well in the past. However, because lessons learned databases are currently highly decentralized, it is often difficult to efficiently and effectively find applicable lessons learned in a form that is useful.

There are many organizations that produce lessons learned. Links to some of these organizations and databases from within and outside the DoD are listed below.

- Center for Army Lessons Learned
- Air Force Center for Knowledge Sharing Lessons Learned
- Center for Systems Engineering at the Air Force Institute of Technology
- Air Force Knowledge Management

- Navy Lessons Learned System
- Joint Center for Lessons Learned
- Department of Energy Lessons Learned
- NASA Lessons Learned Database

4.7. Systems Engineering Resources

4.7.1. Standards and Models

- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 15288, Systems and Software Engineering – System Life Cycle Processes
- ISO/IEC 12207, Systems and Software Engineering – Software Life Cycle Processes
- Electronic Industry Alliance (EIA)/Institute of Electrical and Electronic Engineers (IEEE) J-STD-016, Software Development
- American National Standards Institute (ANSI)/EIA 632, Processes for Engineering a System
- ANSI/EIA-649, National Consensus Standard for Configuration Management
- ANSI/EIA-748A, Earned Value Management Systems
- EIA-859, Consensus Standard for Data Management
- ISO/IEC 26702, Application and Management of the Systems Engineering Process
- CMMI®-DEV, Capability Maturity Model Integration ® for Development
- CMMI®-ACQ, Capability Maturity Model Integration ® for Acquisition
- Best Manufacturing Practices Center of Excellence, Systems Engineering Model

4.7.2. Handbooks and Guides

- Navy Systems Engineering Guide
- INCOSE SE Handbook, A Guide for System Life Cycle Processes and Activities
- MIL-HDBK-61A, Configuration Management
- MIL-HDBK-881A, Work Breakdown Structure
- MIL-HDBK-1785, Systems Security Engineering
- NASA SE Handbook
- DSMC Systems Engineering Fundamentals
- Risk Management Guide for DoD Acquisition
- DoD Guide for Achieving Reliability, Availability, and Maintainability
- Systems Engineering Plan Preparation Guide
- Integrated Master Plan and Integrated Master Schedule Preparation and Use Guide
- Performance Based Logistics: A Program Manager's Product Support Guide

- Designing and Assessing Supportability in DoD Weapon Systems: A Guide to Increased Reliability and Reduced Logistics Footprint
- DoD Template for Application of Total Life Cycle Systems Management (TLCSM) and Performance Based Logistics (PBL) In the Weapon System Life Cycle
- DoD Guide for Uniquely Identifying Items
- The Reliability Analysis Center is a DoD Information Analysis Center, a Center of Excellence, and a technical focal point for information, data, analysis, training and technical assistance in the engineering fields of Reliability, Maintainability, Supportability, and Quality.
- ISO/IEC TR 19760, Systems Engineering – A guide for the application of ISO/IEC 15288 (System Life Cycle Processes)
- Best Manufacturing Practices Center of Excellence, Program Managers' Work Station
- Additional Systems Engineering Guides and Information may be found at the OUSD Acquisition, Technology and Logistics Systems Engineering Center of Excellence
- MIL-HDBK-896, "Manufacturing and Quality Program
- NAVSO P-3687, "Producibility System Guidelines

DEFENSE ACQUISITION GUIDEBOOK
Chapter 5 -- Life-Cycle Logistics

5.0. Overview

5.0. Overview

DoD Directive 5000.01 requires Program Managers to:

> *"develop and implement performance-based logistics strategies that optimize total system availability while minimizing cost and logistics footprint."*

Within the Defense Acquisition Management System, DoDD 5000.01 requires that:

> *"Planning for Operation and Support and the estimation of total ownership costs shall begin as early as possible. Supportability, a key component of performance, shall be considered throughout the system life cycle."*

5.0.1. Purpose

This chapter provides the associated guidance the Program Manager (PM), Product Support Manager (PSM), and Life-Cycle Logisticians can use in influencing the design and providing effective, timely product support capability to achieve the system's materiel readiness and sustain operational capability. Emphasis is placed on integrating life-cycle management principles by using performance-based life-cycle product support strategies to provide effective support. This synchronized with the systems engineering process results in materiel readiness at an optimal life-cycle cost (LCC) by reducing the frequency, duration, and related costs of availability

degrader events to reduce manpower and logistics footprint. An executive summary of key chapter principles is provided below.

The PM, as the life-cycle manager, is responsible for accomplishing program objectives across the life cycle, including the operating & support (O&S) phase. Employing performance-based life-cycle product support tied to sustainment metrics is the overarching Department of Defense (DoD) concept for providing materiel readiness to the user. This logistics aspect of the life-cycle management approach is depicted in Figure 5.0.1.F1 and discussed in subsequent sections.

There are three DoD Decision Support Systems - Joint Capabilities Integration and Development System (JCIDS), Defense Acquisition System, and Planning, Programming, Budgeting and Execution (PPBE) process - that frame the environment for implementing life-cycle management. In addition, there are three related but distinct communities, with corresponding reporting chains, within the DoD -- the acquisition, user, and sustainment chains involved in implementing the decision support systems. Working in tandem these communities share responsibilities which vary depending on the life-cycle phase. Consequently, the PM needs to be involved with each chain. The Defense Acquisition Guidebook focuses on the acquisition chain (e.g. the OSD, Service Secretariat, Program Executive Officer chain, etc.). Chapter 5 addresses the acquisition chain and highlights interfaces with the user chain (e.g. the type commander, Theater Commanders, etc.) and sustainment chain (e.g. supply chain (including the transportation system, maintenance facilities and depots, industrial base), in-service engineering organizations, etc.).

During acquisition the focus is primarily through the acquisition community with requirements input from the user and sustainment communities. It includes the:

- Specification of design parameters for sustainment related system performance capabilities.
- Application of systems engineering to determine the right balance between the system's design requirements and the logistics support requirements to sustain the operational capabilities at an affordable price. This includes using supporting sustainment metrics (e.g. Mean Down Time, Logistics Footprint, etc.) as well as enablers (e.g. condition based maintenance, diagnostics, prognostics, corrosion protection/mitigation, etc.) with their associated metrics to achieve the mandatory sustainment metrics.
- Planning for, resourcing, and executing the design, acquisition, management, and fielding an integrated product support package to sustain the maintenance and support concepts that meet the materiel availability requirements

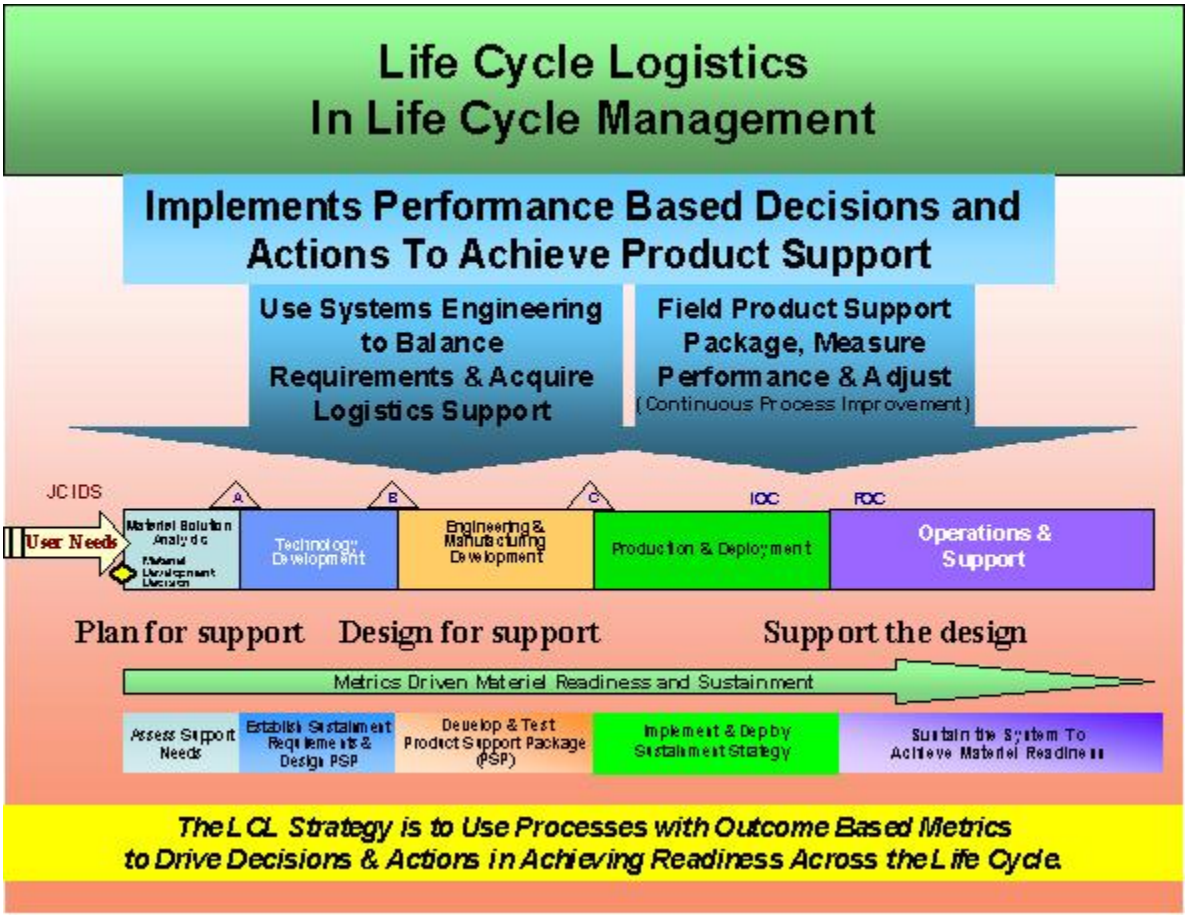


Figure 5.0.1.F1. Life-Cycle Logistics Overview

During operations the focus is primarily through the user and sustainment communities with support from the acquisition community. The PM's focus is on supporting the user's ability to effectively meet mission requirements through the application of systems engineering to implement continuous process improvement initiatives. This involves monitoring performance to identify major readiness degraders (e.g., reliability, cycle time and cost) and to:

- Align and refine the product support package (e.g. the logistics elements) and sustainment processes to achieve the sustainment metrics
- Engage the various communities to achieve optimum materiel readiness
- Optimize or reduce the logistics demand (including the logistics footprint) and support processes (e.g., training, technical data, supply chain, maintenance, etc.) based on actual conditions
- Reduce total ownership costs
- Identify and implement design changes to address evolving requirements, technological obsolescence, diminishing manufacturing sources, or materiel availability shortfalls.

To accomplish this life-cycle product support concept outcomes are estimated in the design phase then measured during testing and operations and become the basis for actions to achieve materiel readiness. The sustainment metrics, including the Sustainment Key Performance Parameter (KPP) with its supporting Key System Attributes (KSAs), provide the common thread to integrate the logistics elements and align the behaviors required to achieve the desired materiel readiness outcome across the entire enterprise. The goal is to use consistent outcome metrics as the basis for actions to provide and sustain affordable materiel readiness across the entire life cycle.

5.0.2. Contents

The information contained in the first three sections of this chapter applies to multiple life-cycle phases in supporting the life-cycle management elements depicted in Figure 5.0.1.F1.

Section 5.1, Life-Cycle Sustainment in the Defense Acquisition Management System, describes life-cycle sustainment, explains its role, and identifies the PM's primary life-cycle logistics and sustainment responsibilities. It provides the context for conducting sustainment-related activities relative to performance-based life-cycle product support and the sustainment metrics. It also addresses intellectual property rights and documentation in contracting.

Section 5.2, Applying Systems Engineering to Life-Cycle Sustainment, focuses on the process to plan for, achieve and sustain affordable systems operational effectiveness. The concept of applying life-cycle cost, modeling & simulation, and supportability analyses to design out "sustainment disablers" to optimize the support system is presented in this section.

Section 5.3, Supportability Design Considerations, focuses on design features that should be incorporated to help make a system more sustainable, including reliability, diagnostic, and predictive monitoring capabilities.

Section 5.4, Sustainment in the Life-Cycle Phases, focuses on how life-cycle sustainment integrates into life-cycle management and the acquisition process/decision points. It identifies key activities in each program phase, whether it is a major new system, a modification to a fielded system, or a redesign of the product support system. This section applies the concepts discussed in sections 5.1, 5.2, and 5.3, placing them in the Defense Acquisition Management System to demonstrate when sustainment related activities take place. It also contains specific focus areas for consideration and the results expected in preparing for each milestone or review.

Section 5.5, References, provides references for further explanation and information.

5.1. Life-Cycle Sustainment in the Defense Acquisition Management System

This section highlights important sustainment related activities and considerations a program manager should carry out. Topics discussed in this section are applicable to multiple phases and it addresses the major deliverables to be prepared or updated during subsequent phases or increments. DoD Instruction 5000.02 provides a complete discussion of the activities and requirements encompassed in the Defense Acquisition Management System. More detailed sustainment related information can be found in subsequent sections and the references.

5.1.1. Life-Cycle Sustainment

5.1.1. Life-Cycle Sustainment

Life-cycle sustainment involves the early planning, development, implementation, and management of a comprehensive, affordable, effective performance driven logistics support strategy. It plays a key role during all phases of the life cycle as Figure 5.1.1.F1 illustrates. The goal is to ensure sustainment considerations are integrated into all planning, implementation, management, and oversight activities associated with the acquisition, development, production, fielding, support, and disposal of a system across its life cycle. This includes:

- Participating in the design process to acquire a highly supportable and sustainable system
- Providing affordable, reliable, effective support strategies and systems that meet the user's requirements with optimum materiel availability
- Developing the appropriate metrics to validate and verify the system engineering design process, and measure the performance of the support strategy/supply chain
- Providing the user effective systems with the minimal logistics footprint (e.g., the measurable size or "presence" of logistics support, including manpower, required to deploy, sustain, and move a system).
- Developing more integrated and streamlined acquisition and statutorily complaint logistics support processes
- Facilitating iterative technology enhancements during the system life cycle

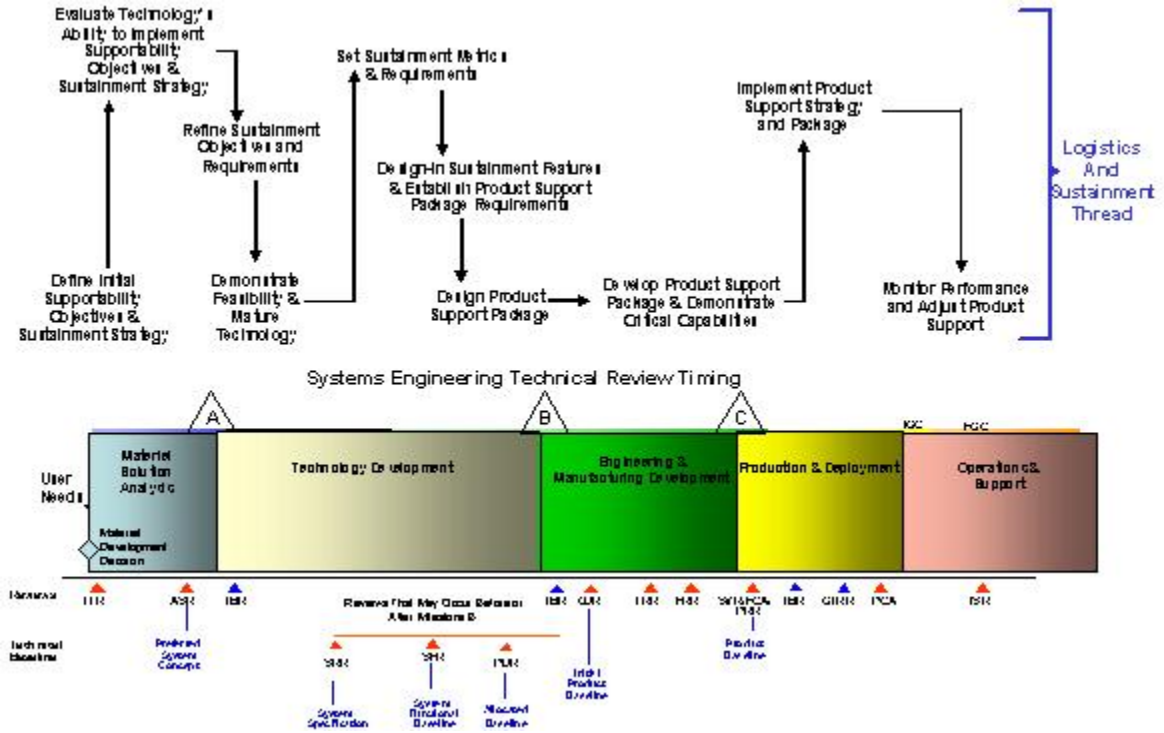


Figure 5.1.1.F1. Sustainment Thread in the Defense Acquisition Management System

The goal can be accomplished by using metrics-driven outcome-based processes to drive decisions and actions by the stakeholders across the enterprise and life cycle. It should be carried out by a cross functional team of subject matter experts ensuring sustainment requirements are both consistently and comprehensively addressed and balanced with cost, schedule and performance. Sustainment should be considered in the systems engineering process to ensure decisions focused on the ability to operate and support a system are implemented during its design, development, production, and sustainment. Key tenets in accomplishing the goal include, but are not limited to:

- Single point of accountability for accomplishing program sustainment objectives including the logistics system and support;
- Incremental acquisition and statutorily complaint product support strategies;
- Comprehensive integration of hardware, software and humans throughout the life cycle to optimize usability, availability, maintainability, sustainability and affordability. This includes follow on modifications to address deficiency reports and sustainment issues.
- Metrics-driven decisions based on a meaningful user outcome measure (e.g., Materiel Availability) supported by a materiel quality measure (e.g., Materiel Reliability), a sustainment quality measure (e.g., Mean Down Time), and a cost measure (e.g., Ownership Cost);
- Understanding industrial base capabilities and service capabilities;

- Ensuring competition, or the option of competition, at both the prime and subcontract level throughout the program life cycle;
- Performance-based life-cycle product support strategies to project and sustain the force with minimal footprint that support the Sustainment KPP, its associated KSAs, and overall affordability goals;
- Continuous process improvement including assessing the life-cycle product support strategies, to include end-to-end sustainment chain planning, assessment, and execution.

5.1.1.1. Product Support

Product Support is the application of the package of integrated logistics elements and support functions necessary to sustain the readiness and operational capability of the system. While it varies by organization typically, the product support package (PSP) includes the logistics elements contained in figure 5.1.1.1.F1. They must be integrated because they impact each other and Materiel Availability. During the acquisition process the focus is on influencing the design for supportability and by fielding the support concept to satisfy user specified requirements for sustaining system performance at the lowest ownership cost. This applies to each increment of capability to be developed. Features include:

- Availability of support to meet Warfighter specified levels of combat and peacetime performance;
- Logistics support that sustains both short and long term readiness;
- Management of life-cycle cost (LCC) through analysis and decision prioritization;
- Maintenance concepts to integrate the logistics elements and optimize readiness while drawing upon both organic and industry sources;
- Data management and configuration management that facilitates cost-effective product support throughout the system life cycle;
- A diminishing manufacturing sources and material shortages management process that ensures effective, affordable, and operationally reliable systems;
- Operator and maintainer training to encompass the full capability of the system.

Developing the **Support Concept** that defines the overall end state is the first step in achieving product support. In developing the support concept, each program should develop an affordable strategy that:

- Positions and delivers materiel to satisfy highly variable readiness and combat sustainment needs in a variety of unique and demanding environments.
- Meets all materiel management and maintenance statutory requirements.
- Supports rapid power projection.
- Improves readiness through performance-based sustainment strategies.
- Establishes end-to-end processes focused on outcomes.
- Implements contemporary business systems and practices that enable the integration of people, information, and processes.

- Protects critical program information including as it moves through the supply chain, as required in DoD Instruction 5200.39.

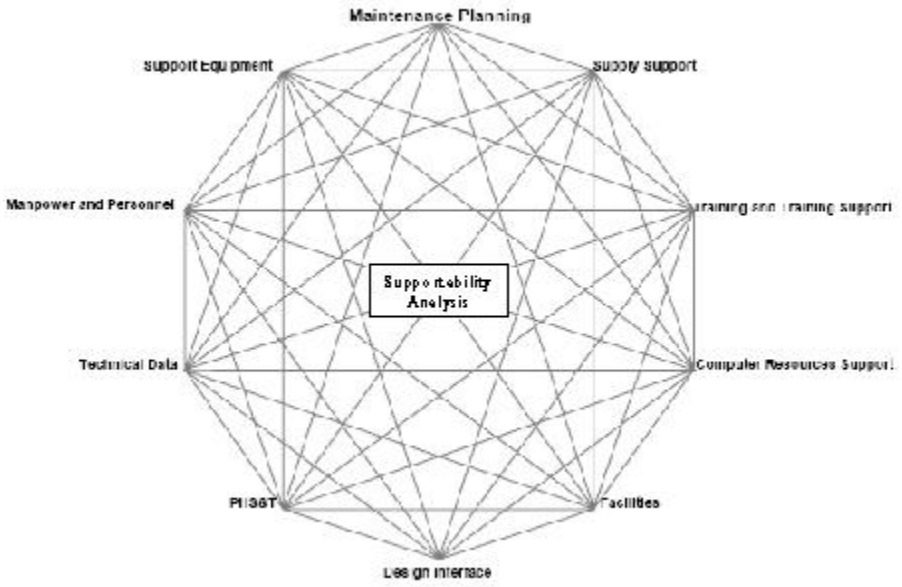


Figure 5.1.1.1.F1. PSP Logistics Elements

The support concept has to address the hardware and its associated software (including Commercial Off The Self (COTS) software) since software can be a major sustainment issue as systems become more software intensive. Programs need to plan for technology refreshment and maintaining the software after production. This includes how changes (for obsolescence/ technology refreshment and maintaining the software) will be budgeted and executed along with the necessary technical data required to sustain the software throughout the system life. In addition to sustaining the software, aspects such as customer support, systems administration help desk support, etc. need to be considered.

Achieving the support concept and sustaining operational capability requires the involvement of the logistics, engineering, testing, program management, contracts, supply chain, and financial management experts. The overall support strategy, documented in the Life-Cycle Sustainment Plan, should include life-cycle support planning and address actions to assure sustainment and continually improve product affordability for programs in initial procurement, re-procurement, and post-production support. A performance-based product support process will be used to align the support activities necessary to meet these objectives.

5.1.1.2. Sustainment Metrics

In a performance based environment, sustainment related specifications, with a specified range of minimum mandatory (threshold) and target (objective) performance capability design parameters are established with accompanying metrics covering the entire enterprise. This includes the system and the supply chain supporting it. (The same basic model holds for the supply chain, but this chapter focuses on the program manger's role.) Sustained materiel readiness of war fighting capability can then be achieved by developing optimally effective and affordable total ownership costs investment strategies to achieve the sustainment metrics. The metrics should possess the following key attributes.

Traceable to User Requirements: The sustainment metric requirements must reflect user requirements. The metrics and their values should be derived from the systems operational requirements/use (as articulated in the Capabilities-Based Assessment (CBA) process) and the planned logistical support strategy to sustain it. They should also be supported by comprehensive and early supportability planning and analyses to balance technology feasibility, life-cycle costs and operational needs.

Achievable and Verifiable: The sustainment metric requirements must be obtainable. (Unrealistic requirements adversely affect the development process, result in unachievable performance levels, and drive higher acquisition and sustainment costs.) They should also be stated in demonstrable terms reflecting the projected range of military operations (e.g., design reference missions) and intended operating environment that must be supported. These attributes are critical for sustainment requirements to be used within the design tradeoff process along with cost, schedule, and performance.

Minimum Reporting: The specific metrics should be tailored to the program and its operational and sustainment needs. At a minimum, they should consist of four interrelated metrics: an outcome metric meaningful to the user in achieving and sustaining the operating tempo; a materiel metric to measure the system's quality; a response metric to measure the quality of the logistics system; and a cost metric. They should be consistently defined within the program and traceable to the operational need. At the top level, the sustainment metrics should focus on providing an effective system that is available and reliable with minimal down time at a reasonable cost. Exact definitions and details can be found in the JCIDS Manual. However, programs have the flexibility to tailor the metrics (including adding additional sustainment metrics (e.g. footprint, manning levels) as long as the intent is met. The following describes the general intent of each of the metrics:

- **Materiel Availability** – the percentage of the total inventory (not just the operationally assigned assets) operationally capable at a given time based on materiel condition. This "total inventory" aspect is critical because it not only measures the ability to execute "today's" missions but also provides an indication of the "surge" ability. Materiel availability is primarily an indication of the percentage of time a system is operationally capable of performing an assigned mission. In addition to the planned missions/scenarios, operating tempo, and sustainment concept of operations (CONOPS), this metric is

dependent on system reliability and the mean downtime resulting from, but not limited to failures, scheduled downtime, general maintenance or servicing actions.

- **Materiel Reliability** - the probability the system will perform without failure over a specific interval. This metric focuses on reliability of the entire system and should not be confused with the mission success rate. Defining the criteria for measuring relevant failures (including consistent definitions for failures (e.g., criteria for counting assets as "up" or "down") and mission critical systems) and clearly defining how time intervals will be measured are important and must be consistent with the other metrics.
- **Mean Down Time** - the average time an end item is unavailable to perform its assigned mission after it experiences unscheduled or scheduled maintenance actions. It includes all time where the system is not at the disposal of the Force Provider to initiate missions. In addition to the projected supply chain approach with its resultant logistics footprint, the impact of surge/deployment acceleration requirements should be determined for this and the Materiel Availability metric.
- **Ownership Cost** - a subset of the total ownership cost, focusing on the operations and support cost. The objective is to use ownership costs to influence program design, acquisition, and sustainment alternative decisions. The cost elements considered vary over the system life cycle so it is important the cost model be consistent with the design specifications as well as the assumptions and conditions used for Materiel Availability, Materiel Reliability and Mean Down Time metrics. In the early acquisition stages, total ownership costs need to be considered in the trade decisions. For example, even though manpower is not one of the mandatory Ownership Cost reporting elements, it is important especially early in the life cycle and needs to be considered. This is because manpower decisions drive a host of other human related tradeoffs and associated ownership costs for the system (e.g. training, personnel selection, interface design considerations). However, once manpower decisions have been made, the focus is on the materiel ownership costs with relevant total ownership cost considerations handled by appropriate burdened cost factors. Consequently, it is important the cost structure being used be clearly defined (along with the cost estimating relationships/models, and assumptions) and all relevant costs for the trade-off decisions are included regardless of funding source. (see chapter 3).

The selection of the specific performance metrics should be carefully considered and supported by an operationally-oriented analysis, taking into account technology maturity, fiscal constraints, and the timeframe the capability is required. In implementing performance-based life-cycle product support strategies, the metrics should be appropriate to the scope of product support integrators and providers responsibilities and should be revisited as necessary to ensure they are motivating the desired behaviors across the enterprise. During operations the program can consider measuring additional metrics for configuration control, training effectiveness, overall user satisfaction, etc. The specific metrics selected should tie to existing user performance measures and reporting systems. In addition, existing logistics and financial metrics should be related to these top level user performance metrics and considered as supporting metrics to help provide confidence they can be met as well as identify risk areas.

5.1.1.3. Performance-Based Life-Cycle Product Support Implementation

DoD Directive 5000.01, E1.1.17, requires program managers (PMs) to:

> *"develop and implement performance-based product support strategies that optimize total system availability while minimizing cost and logistics footprint. Sustainment strategies shall include the best use of public and private sector capabilities through government/industry partnering initiatives, in accordance with statutory requirements."*

Building on the best features of the public and private sectors is a key component of the support strategy. The Performance-Based Life-Cycle Product Support Implementation Framework (Figure 5.1.1.3.F1) captures the range of capability solutions that could be employed. The framework is incremental, in that each alternative builds on the previous category. In all cases the system's sustainment parameters are projected and measured during the design process and then re-assesses once the system is operational so appropriate actions can be taken to achieve the Materiel Availability objective. Within each category, the program manager is responsible for working with the stakeholders to ensure the appropriate actions are taken to meet the user's needs. The difference is the amount of financial risk shared with the product support integrator or provider and sustainment aspects covered. The categories do not imply a level of "goodness" but only provide a means to illustrate the wide range of implementation options available to the program. Each category description is described below.

Category 1: In a life-cycle management environment, all programs should perform to at least this level. This is the traditional support concept where the program buys the various individual support elements. The government develops the requirements, integrates, procures, and balances the logistics elements to achieve the material availability outcome. The contractor metrics are usually cost and schedule. The difference from the traditional approach is what happens once the system is operational. Once operational, the program manager measures the materiel availability and takes appropriate actions with the stakeholders to meet the user's needs. However, most of the fiscal risks are on the government side and the PM works with the logistics element functional offices, government infrastructure/supply chain, and contractors to determine and ensure corrective actions are taken.

Category 2: At level 2 fiscal risks begin to transition, but only in narrow but critical supply chain functional areas. Typical functions falling within this level include providing material, inventory management, transportation, and/or maintenance where the provider is accountable for the responsiveness required to meet customer requirements. This level generally concentrates on providing parts with the government making design decisions. Part availability, mean down time (MDT) or logistics response time (LRT) are the typical metrics for Level 2 implementations where the time it takes the supplier to deliver the part, commodity or service to the user determines their payment. In using the approach, care must be given to the requirements and

contract terms to ensure they drive the supplier's behavior so the government achieves an affordable material readiness outcome.

The PM is still responsible for taking the appropriate actions with the providers; however, more risks are shared because there are fewer providers with whom to coordinate. The PM still procures many of the individual logistics elements and manages the systems configuration. The program has to develop performance requirements, integrate, procure, and balance the elements not included in the Performance-Based Agreement (PBA) to achieve an affordable materiel availability outcome.

Category 3: This level expands the provider's fiscal risk level by transferring life-cycle support activities to the product support integrator (PSI), making them accountable for sustaining overall system materiel availability. Category 3 typically focuses on maintaining the required availability of key components or assemblies, such as a wing flap or auxiliary power unit, but can include the entire system. In Category 3, there is an additional PSI focus on life-cycle support, training, maintenance, repair and overhaul including logistics planning and execution, in-service engineering, configuration management and transportation. In Category 3, the PSI may also make repair vs. replace decisions. The preferred metric is materiel availability.

At this level the product support integrator is assigned specific life-cycle responsibility, solely or in partnership, for the breadth of processes affecting materiel availability. This includes aspects of sustainment engineering and configuration control, since reliability and maintenance of equipment and effectiveness of the supply chain influences continually affordable operational availability.

Category 4: This level transfers life-cycle support and design performance responsibilities making the product support integrator responsible for assuring operational availability (Ao) or operational capability. Typically this level applies to systems in the form of operational capability, such as "steaming hours, flying hours or miles per month"; "launches per month"; "power by the hour"; etc. The PSI is assigned responsibility, solely or in partnership, for the breadth of processes that influence Materiel Readiness. This gives the PSI the flexibility to adopt any practices and technology enablers needed to meet required performance levels, including the number of systems deployed and where they are located or staged.

Performance-Based Product Support Contracts (PBL): The DoD intent is to use performance-based support. This includes, where it provides the best long term value, using performance based contracts rather than transaction based contracts (i.e. buying Materiel Availability vice buying spares or support equipment). Any best value assessment has to consider not only cost, but also all other quantifiable and non-quantifiable factors associated with any resultant investment decision. The assessment should stand on its own and be able to withstand rigorous analysis and review by independent audit agencies. PMs should strive for the right mix of implementation in terms of functions provided and the extent to which they are applied to the system.

Contracting for performance based logistics is a multiple step process that can be applied to new, modified or legacy systems. The process is detailed on the web-based PBL Toolkit found at https://acc.dau.mil/pbl as a best practice. It is a proven process focusing on legacy programs that can be tailored and adapted to individual systems, subsystems or components to meet its needs and its business and operational environments.

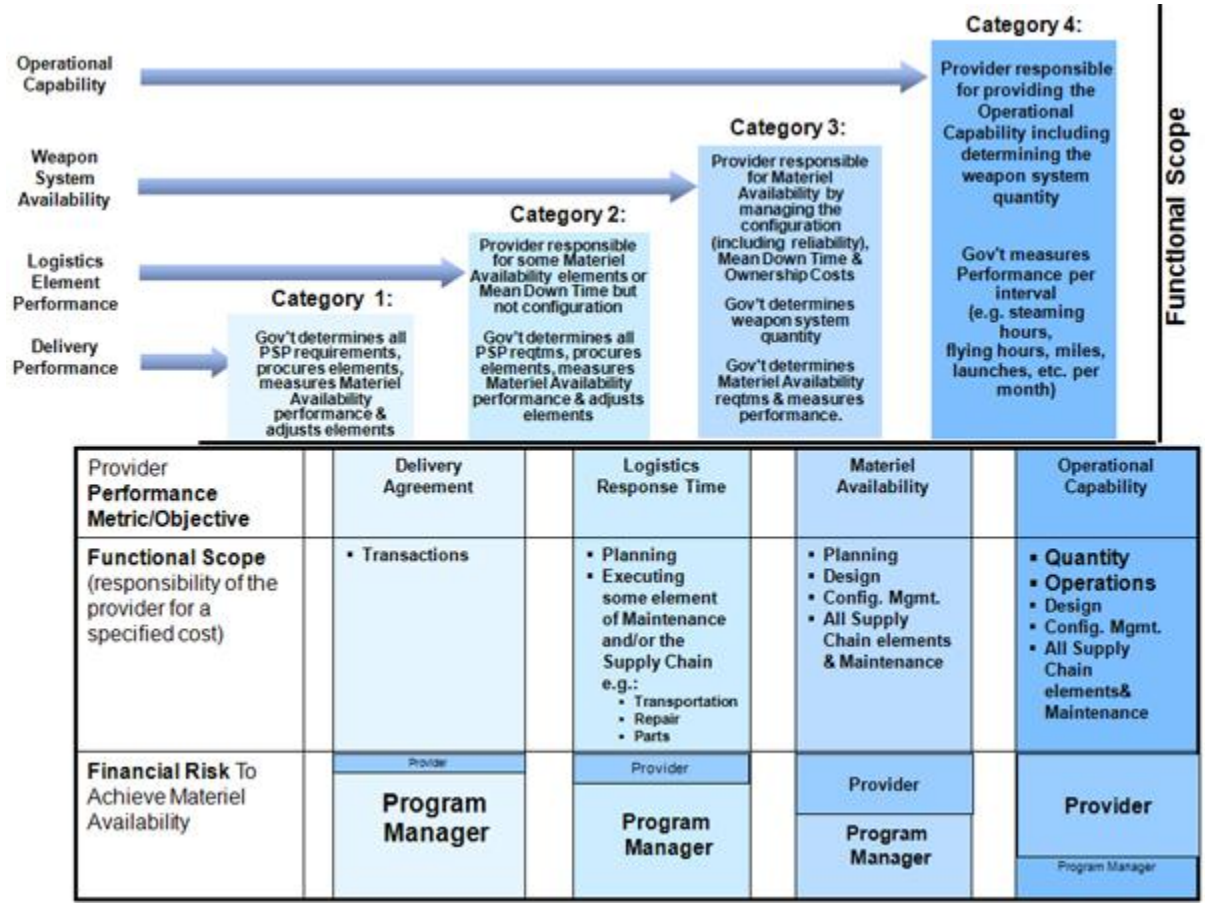


Figure 5.1.1.3.F1. Performance-Based Life-Cycle Product Support Implementation Framework

5.1.1.4. Sustaining System Performance

Conditions change over the life of any system so it is critical that performance be measured against a plan and appropriate steps be taken as conditions warrant. These steps can range from corrective actions anywhere within the program or its supply chain to re-baselining the metrics. Care should be taken to ensure the appropriate stakeholders are involved with any requirements change decisions and that the baseline is not changed too often to avoid rubber baselines.

Monitoring actual performance (or projected performance during design) then taking the appropriate corrective actions when needed is critical in achieving and sustaining performance. During testing, monitoring allows early corrective actions before the system is deployed. During operations, it can help the PM determine if the metrics are driving the desired behaviors (or if different metrics are needed) to achieve the desired behavior or performance. Consequently, the PM should have a strong monitoring and assessment program structured to fit the unique program conditions. Representatives from each of the functional areas that drive the metrics should be involved in the process.

The Condition Based Maintenance Plus (CBM+) is a specific initiative which can be useful in cost effectively sustaining performance. It is the application and integration of appropriate processes, technologies, and knowledge-based capabilities to improve the reliability and maintenance effectiveness of DoD systems and components. At its core, CBM+ is maintenance performed based on evidence of need provided by Reliability Centered Maintenance (RCM) analysis and other enabling processes and technologies. CBM+ uses a systems engineering approach to collect data, enable analysis, and support the decision-making processes for system acquisition, sustainment, and operations. CBM+ policy is established in DoD Instruction 4151.22.

The program team can often be too close to the day-to-day decisions, so independent program reviews can be useful in helping ensure the system will be able to maintain or improve performance. The DoD components each have their own structures to do this, usually tied to formal program reviews, but the PM should consider bringing in their own independent reviewers to help in the process and gain lessons learned from other programs.

5.1.2. Life-Cycle Sustainment and the DoDI 5000.02 Acquisition Environment

5.1.2. Life-Cycle Sustainment and the DoDI 5000.02 Acquisition Environment

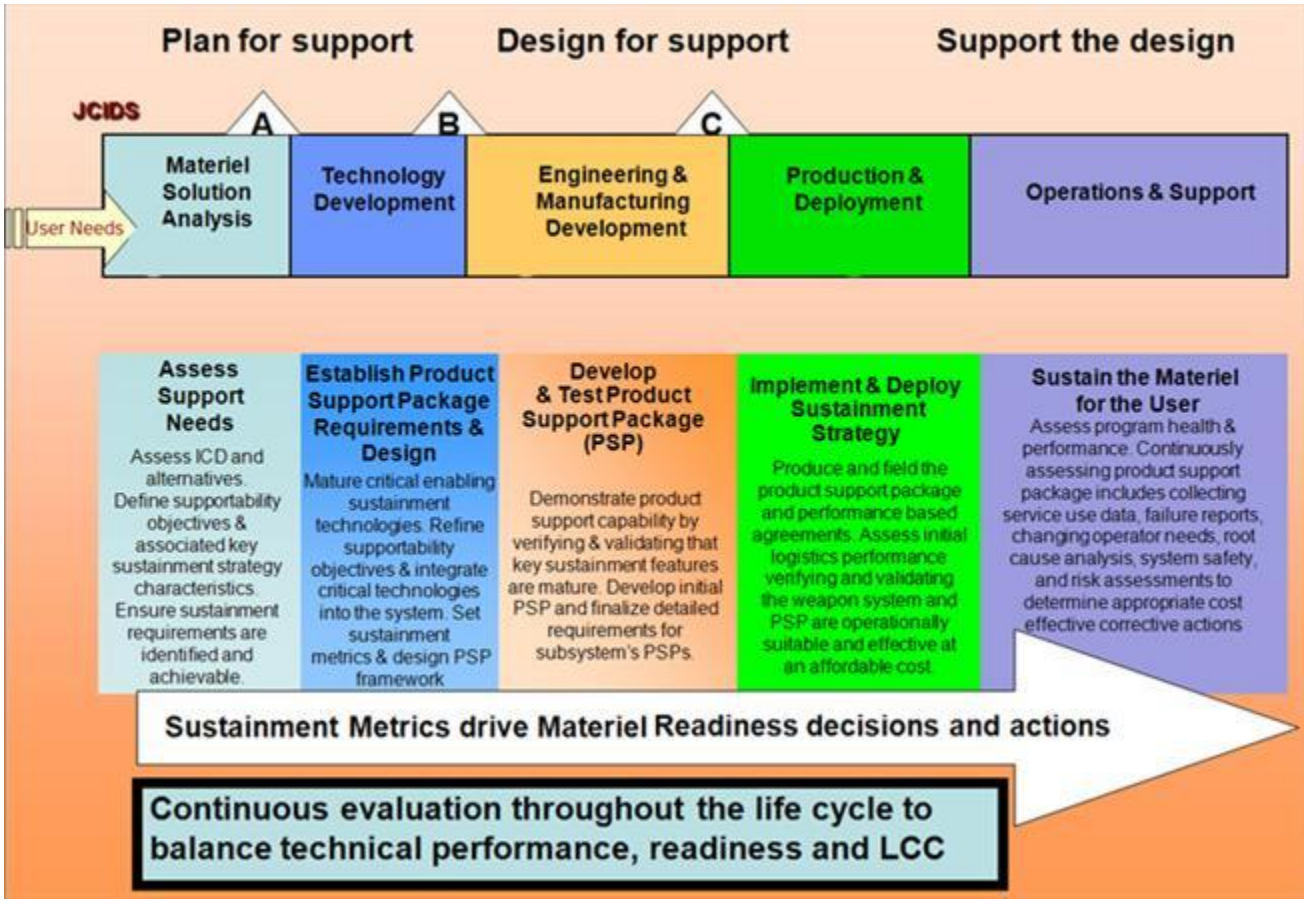
Acquisition programs are structured in phases separated by milestone decisions in accordance with the Life-Cycle Management System established in DoD Instruction 5000.02. (An on-line, interactive version of the Integrated Defense Acquisition, Technology, and Logistics Life-Cycle Management System is also available.) In each phase, from defining user needs to disposal, there are important sustainment issues and actions to address. Figure 5.1.2.F1 provides an overview of key sustainment activities by phase. In addition, under the evolutionary acquisition strategy, each block should address support implications. In those cases a thorough assessment of the existing support strategy vis-à-vis any new sustainment requirements should be conducted to ensure the

support implications for each block are understood, and changes are made as necessary, to ensure an affordable materiel readiness strategy.

Statutory, Policy, and Guidance Factors. While the PM has latitude in developing the acquisition strategy, there are statutory requirements that must be taken into account. Congress has enacted a number of statutes capabilities to assure availability of a ready and controlled (i.e. government owned) source of technical competence and resources to ensure effective and timely response to a national defense contingency requirement (10 USC 2464) and ensure that there is a balance between the private and the public sector industrial base (10 USC 2466 and 10 USC 2474). The support strategy must ensure compliance with all statutory and regulatory requirements. These legislative and statutory issues must be considered as an integral and evolving aspect of all Life-Cycle Management decisions. The PM must also follow Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) guidance, as well as appropriate DoD Directives and Instructions. Instructions, including the DoDD 4151.18 (Maintenance of Military Materiel), DoDI 4151.19 (Serialized Item Management (SIM) for Materiel maintenance), DoDI 4151.22 (Condition Based Maintenance Plus (CBM+) for Materiel Maintenance), DoDI 8320.04 (Item Unique Identification (IUID) Standards for Tangible Personal Property) need to be addressed.

Support strategy. PMs balance multiple objectives in designing the strategy to achieve operational effectiveness while maintaining affordability. PMs accomplish this by laying out and executing a support strategy so every part of the product support package is integrated and contributes to the user's mission capability. To ensure there is a means to assess performance the PM and product support provider(s) should redefine and augment system sustainment metrics used to meet system capability requirements. (Support providers may be public, private, or a mix, to include public private partnerships. Examples of public support providers include DoD maintenance depots, DoD Component and Defense Logistics Agency (DLA) inventory control points and distribution depots.) The PM and the support provider(s) should enter into Performance-Based Agreements that define the sustainment metrics necessary to meet the system performance requirements.

A program manager's best means of ensuring a system will meet its sustainment objectives and satisfy user sustainment needs, is to ensure sustainment considerations are infused in all phases of the program's life cycle. It is especially important that sustainment considerations are included in Pre-Systems Acquisition and Acquisition activities, including the Joint Capabilities Integration and Development System (JCIDS) process, structured program reviews, and tracking sustainment performance drivers during Test and Evaluation. Even after the Initial Operational Capability (IOC) date, the support strategy should be periodically reviewed and revised when sustainment metrics are not being met or requirements change. These actions should be defined in the Life-Cycle Sustainment Plan (LCSP) and other appropriate program documents.



5.1.2.1. Key Program Documents

This section addresses the sustainment aspects that should be included in key program acquisition documents that cut across life-cycle phases. (Phase unique documents and focus areas are addressed in subsequent sections). To help ensure a shared understanding of the program's intent, it is important the documents used by the PM in the acquisition process and program reviews be updated during subsequent phases, especially prior to milestone decisions.

Initial Capabilities Document (ICD) / Capability Development Document (CDD) / Capability Production Document (CPD). These documents are the sponsor's means to specify authoritative and testable, performance capabilities for the program. The ICD prefaces a system materiel decision and evolves into the CDD, which prioritizes KPP and subset KSA performance capability design and development parameters. The baseline CPD is finalized after the system level Critical Design Review and before Milestone C. In addition to supportability related KPP/KSAs, the ICD, CDD, and CPD narrative should also address the following:

- System maintenance/support concepts and usage scenarios

- Operational and support environments. This should include the general support categories relative to the logistics support infrastructure (remote sites, organic depots, commercial facilities, air bases or ship yards, etc. without naming specific locations)
- Expected durations of support
- Support or maintenance effectiveness metrics and key enablers, such as diagnostics/ prognostics
- Conditions conducive to joint sustainment and to performance-based support strategies

Analysis of Alternatives (AoA) . The AoA should describe and include the results of the supportability analyses and trade-offs conducted to determine the optimum support concept as part of the preferred system concept. It should also include the assumptions used in the analyses.

Technology Development Strategy (TDS) . The TDS should also include the specific new sustainment related technologies required to achieve the Sustainment KPP/KSAs. Specific emphasis should be placed on technologies required to achieve logistics performance (including reliability) over what is currently achieved in today's operational environment.

Acquisition Program Baseline (APB) . The APB documents the performance requirements, schedules, and program cost funding and estimates. The program sponsor and program manager will ensure content includes Sustainment KPP/KSAs parameters, measurement metrics, and all programmatic direction affecting life-cycle support strategy planning and execution.

Acquisition Strategy . The Acquisition Strategy describes the PM's approach for acquiring the system and its support. The program manager must include the acquisition strategy for achieving the sustainment metrics and acquiring the product support package. The Acquisition Strategy should include the Life-cycle Sustainment Plan content, focusing on key upcoming actions and the timeline to acquire the logistics elements necessary to maintain the system's readiness and operational capability. This includes reducing the maintenance burden, reducing the supply chain (both the commercial and organic supply chain) and minimizing the footprint through deliberate design techniques for both the weapon system and the support system. Specifically, it should address how the product support package required to support the materiel management, distribution, technical data management, support equipment, maintenance, training, configuration management, engineering support, supply support, and failure reporting/analysis, functions will be acquired. It should also include a summary of the approach for acquiring key enablers for achieving the sustainment metrics (e.g., using diagnostics, prognostics, modular open systems approach, reliability growth).

Test and Evaluation Master Plan . Proper testing is critical to achieve the sustainment metrics thresholds and objectives. The program manager should therefore ensure the TEMP includes a description of the requirements and test points/methods for each of them as well as any appropriate enabler or logistics consideration.

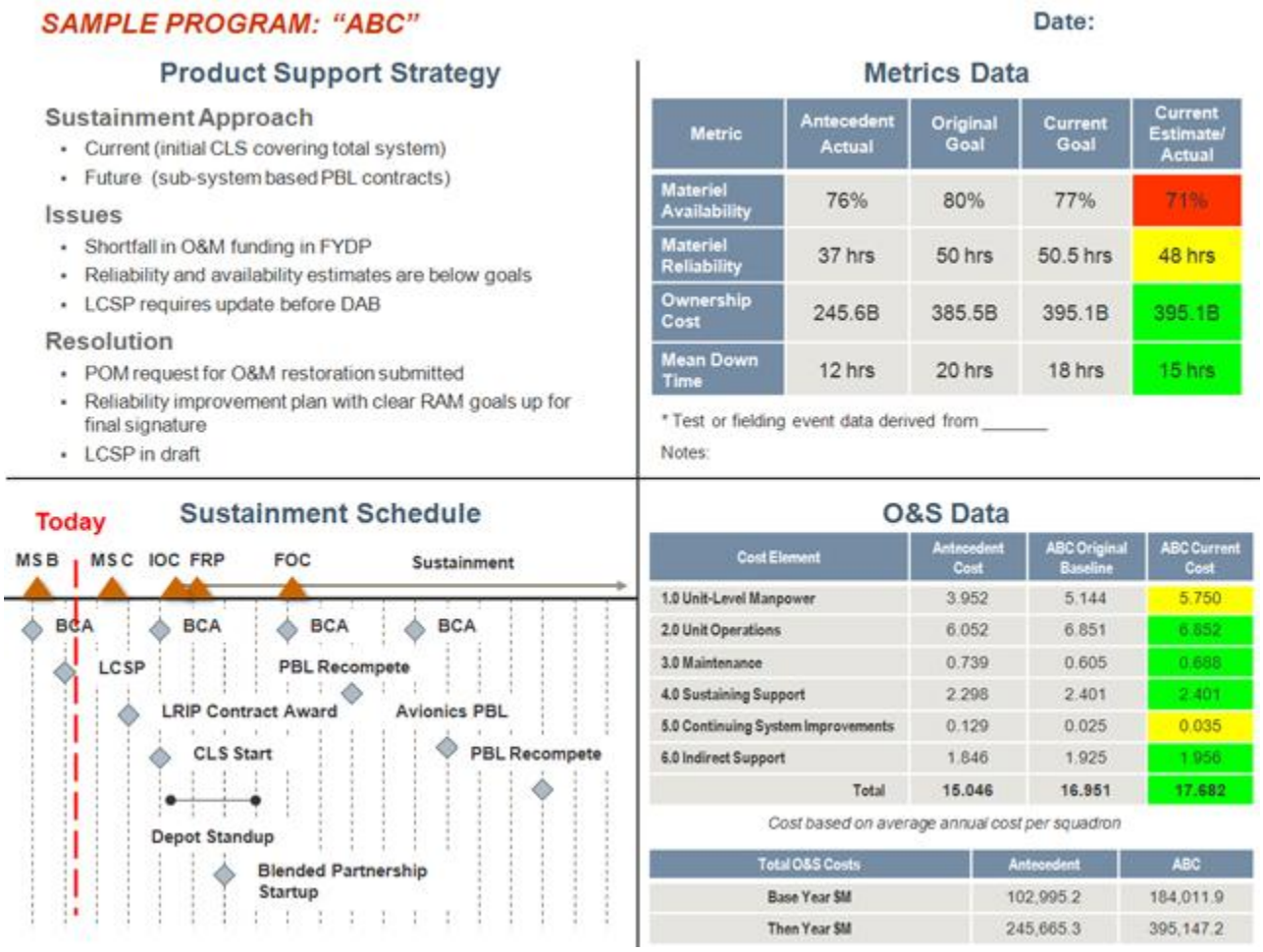
Systems Engineering Plan . The systems engineering approach is an integral part in designing for sustainment and supporting the design. (See the Systems Engineering Preparation Guide.)

Accordingly, in developing and updating the SEP, the PM should integrate sustainment into the program's technical approach described by addressing how the:

- Sustainment metrics are to be integrated and managed with other requirements.
- Maintenance, sustainment and other support personnel aspects included in the HSI plan / process will be integrated with the Systems Engineering Process.
- Program will organize and staff its Integrated Product Teams (IPTs) to address sustainment.
- Process for ensuring sustainment is considered, including the development and update of the Failure Mode, Effects & Criticality Analysis (FMECA) matrix; identification of critical safety items (CSIs); Failure Reporting, Analysis & Corrective Action System (FRACAS); and trend analysis for maturation purposes of the system and its support system.
- Technical baselines (functional, allocated, and product) will address the end item system and its product support package elements.
- Technical reviews will be used to define and assess sustainment and product support package technical maturity against the baselines. This is important because the reviews provide opportunities to ensure sustainment features are being designed into the system. They also provide the opportunity to assess the supportability design feature's maturity so the product support package can be adjusted as needed to achieve the sustainment metrics.

Diminishing Manufacturing Sources/Materiel Shortages (DMSMS) Plan. An efficient, proactive DMSMS management process is critical to providing more effective, affordable, and operational systems by proactively identifying and mitigating DMSMS issues that affect their availability and supportability. Actively addressing DMSMS concerns throughout the entire life of the program will help ensure effective life-cycle support and reduce adverse impacts on readiness or mission capability. The DOD DMSMS Guidebook (SD-22) provides a compilation of the best proactive practices for managing the risk of obsolescence. Establishment of the DMSMS program and proper planning during design will ensure successful implementation in sustainment and throughout the life cycle.

Sustainment Quad Chart. The Quad chart provides sustainment related information in a standardized format (Figure 5.1.2.1.F1) that ACAT 1D PMs shall use in reporting status at Overarching Integrated Product Team (OIPT) and Defense Acquisition Board (DAB) reviews. It is used to strengthen sustainment governance by providing senior management visibility of key sustainment factors to help ensure the PM’s sustainment strategy is meeting the Warfighter materiel readiness objectives with long-term affordability considerations. Reporting begins at program initiation and continues through each subsequent milestone, the production decision, and at other reviews when directed. (Detailed instructions for how to fill out the chart can be found at https://acc.dau.mil/CommunityBrowser.aspx?id=360876&lang=en-US).



SAMPLE PROGRAM: "ABC"

Date:

Product Support Strategy

Sustainment Approach

- Current (initial CLS covering total system)
- Future (sub-system based PBL contracts)

Issues

- Shortfall in O&M funding in FYDP
- Reliability and availability estimates are below goals
- LCSP requires update before DAB

Resolution

- POM request for O&M restoration submitted
- Reliability improvement plan with clear RAM goals up for final signature
- LCSP in draft

Metrics Data

Metric	Antecedent Actual	Original Goal	Current Goal	Current Estimate/ Actual
Materiel Availability	76%	80%	77%	71%
Materiel Reliability	37 hrs	50 hrs	50.5 hrs	48 hrs
Ownership Cost	245.6B	385.5B	395.1B	395.1B
Mean Down Time	12 hrs	20 hrs	18 hrs	15 hrs

* Test or fielding event data derived from _____

Notes:

Today

Sustainment Schedule

MS B MS C IOC FRP FOC Sustainment

BCA BCA BCA BCA

LCSP

PBL Recompete

LRIP Contract Award

Avionics PBL

CLS Start

PBL Recompete

Depot Standup

Blended Partnership Startup

O&S Data

Cost Element	Antecedent Cost	ABC Original Baseline	ABC Current Cost
1.0 Unit-Level Manpower	3.952	5.144	5.750
2.0 Unit Operations	6.052	6.851	6.852
3.0 Maintenance	0.739	0.605	0.688
4.0 Sustaining Support	2.298	2.401	2.401
5.0 Continuing System Improvements	0.129	0.025	0.035
6.0 Indirect Support	1.846	1.925	1.956
Total	15.046	16.951	17.682

Cost based on average annual cost per squadron

Total O&S Costs	Antecedent	ABC
Base Year $M	102,995.2	184,011.9
Then Year $M	245,665.3	395,147.2

Figure 5.1.2.1.F1. Sustainment Chart

5.1.2.2. Life-Cycle Sustainment Plan (LCSP)

DoD Instruction 5000.02 requires that a LCSP be developed and included as a part of the Acquisition Strategy to document how the sustainment strategy is being implemented. (Currently the DoD Components use different names to address this requirement, e.g., the Army's Supportability Strategy, the USAF's Life-Cycle Management Plan.) Regardless of the name, the LCSP documents the Program Manager's plan for formulating, implementing and executing the sustainment strategy so that the system's design as well as the development of the product support package (including any support contracts) are integrated and contribute to the Warfighter's mission requirements by achieving and maintaining the Sustainment KPP/KSAs. The LCSP is a living document describing the approach and resources necessary to develop and integrate sustainment requirements into the system's design, development, testing & evaluation, fielding and operations. The LCSP should be tailored to meet program needs documenting the current program plan in the following areas:

- The maintenance and support concepts
- How the sustainment metrics will be achieved and sustained throughout the life-cycle
- How sustainment is addressed as an integral part of the program's acquisition strategy and system design process
- The assigned responsibilities and management approach for achieving effective and timely acquisition, product support, and availability throughout the life-cycle including the Program Manager's role in planning for and executing sustainment
- The funding required and budgeted by year and appropriation for the main sustainment cost categories including operating & support costs
- The plan for identifying and selecting sources of repair or support
- The sustainment risk areas and mitigation plans
- Product support implementation status
- Results and recommendations from DoD Component Independent Logistics Assessments (ILA)

Figure 5.1.2.2.F1 provides the outline that should be used to document the PM's plan for how the Product Support Manger will implement the sustainment strategy. Details for each section can be found at the LCSP web site.

Executive Summary

1.0. Introduction

1.1. Program Overview

2.0 Sustainment Concept

2.1. Sustainment Drivers

2.2. Sustainment Partnering

3.0 Sustainment Performance Requirements

3.1 Acceptance Criteria

3.2 Testing and Demonstrating Sustainment Requirements

4.0 Sustainment Acquisition Strategy

5.0 Sustainment Design Characteristics

6.0 Product Support Package Status Overview

12.4 Manpower and Personnel

12.4.1 System Operator Requirements

12.4.2 System Maintainer Requirements

12.4.3 Human System Integration (HSI)

12.5 Support Equipment (SE)

12.6 Supply Support

12.6.1 Parts and Material Trade Studies and Selection Process

12.6.2 Supply Chain Management

12.6.3 Provisioning of Initial and Follow-On Spares

12.6.4 Managing Supply Chain Risks

12.7 Facilities

12.8 Packaging, Handling, Storage, and Transportation (PHS&T) Requirements

12.9 Maintenance and Repair Capabilities

13.0 Other

Figure 5.1.2.2.F1. LCSP Outline

LCSP Development. Life-cycle sustainment planning and execution seamlessly span a system's entire life-cycle evolving over time (see Figure 5.1.2.2.F2). The LCSP begins in the Materiel Solution Analysis Phase by describing the notional product support and maintenance concepts used to determine the sustainment requirements optimizing readiness outcomes and minimal life cycle-cost. After Milestone A the LCSP evolves from a strategic outline to a management plan describing the sustainment efforts in the system design and acquisition processes to achieve the required performance and sustainment outcomes necessary to ensure required Warfighter capabilities. It evolves at Milestone B into a detailed execution plan for how the product support package is to be designed, acquired, sustained, and how sustainment will be applied, measured, managed, assessed, modified, and reported from system fielding through disposal. The LCSP is submitted with the Acquisition Strategy prior to Milestone B and the Executive Summary is included in the Acquisition Strategy.

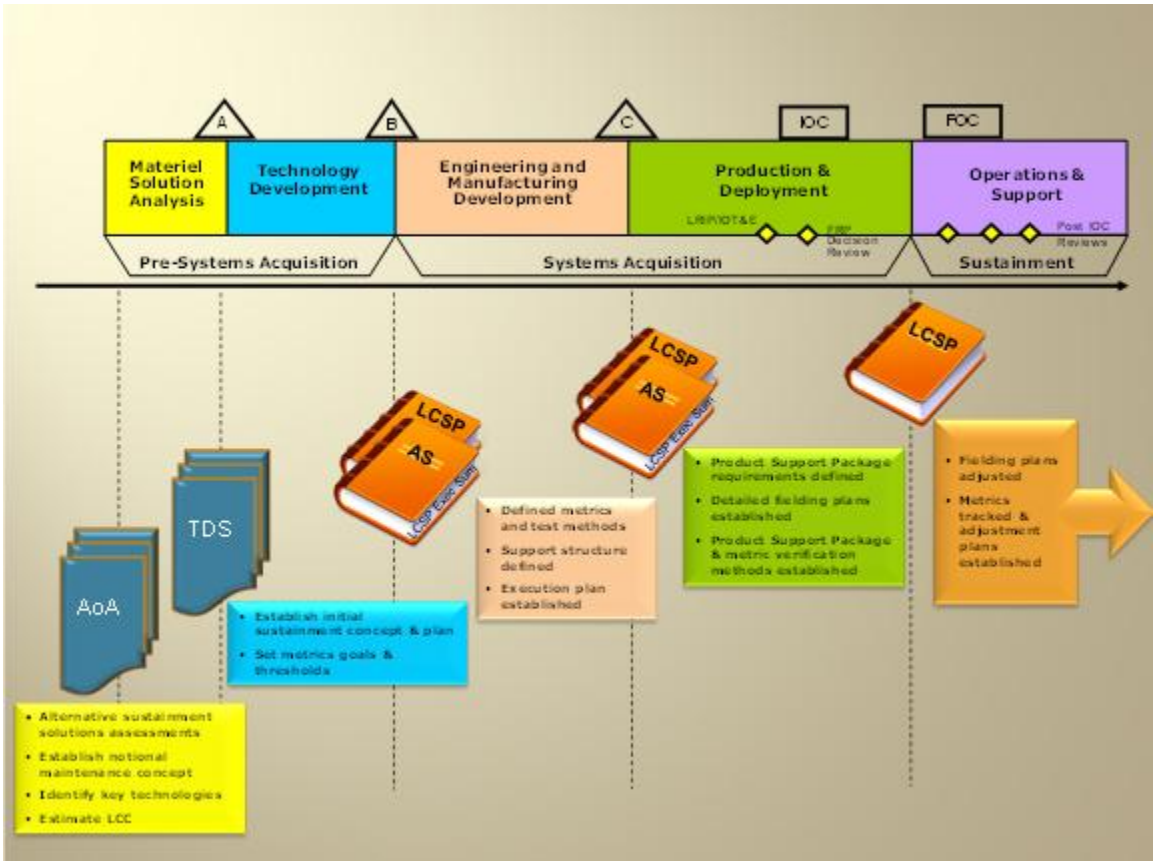


Figure 5.1.2.2.F2. LCSP Evolution

By Milestone C, the LCSP describes the content and implementation status of the product support package (including any sustainment related contracts, e.g. Interim Contractor Support, Contractor Logistics Support) to achieve the Sustainment KPP/KSAs. In addition to sustaining the system performance capability threshold criteria and meeting any evolving user readiness needs, the LCSP details how the program will manage O&S costs and reduce the logistics footprint. After the Full Rate Production Decision Review update, the LCSP describes the plans for sustaining affordable materiel availability as well as accommodating modifications, upgrades, and re-procurement. It should be updated for any Post-IOC Sustainment Reviews and shall be updated, at a minimum every 5 years, or when:

- Subsequent increments are approved and funded to reflect how the support strategy will evolve to support multiple configurations
- Significant changes are required to the product support package to achieve the objective sustainment metrics including major support provider changes.

As the program matures, the LCSP is updated to reflect increasing levels of detail as they become available. The detail and focus will vary depending on the life-cycle phase but in all cases the information should be in sufficient depth to ensure the acquisition, design, sustainment, and user communities have an early common understanding of the sustainment requirements,

approach, and associated risks. Figure 5.1.2.2.1.F3 provides the minimum focus areas that should be incorporated regardless of the phase. Figure 5.1.2.2.1.F4 provides a cross reference as to where each of the focus areas should be documented in the LCSP. Section 5.4 expands on the primary focus areas for each life-cycle phase.

1. Current Program Description - Describes how sustainment considerations are being implemented in the program.

1.1 Sustainment and Maintenance Concepts - Overview of the program support strategy

1.2 Sustainment Acquisition Strategy - Overview of sustainment/logistics contracts (including the extent to which it is traditional transaction based/process focused and performance based/outcome focused)

1.3 Sustainment Funding/Budget - Program funding (by colors of money) to implement the sustainment strategy

1.4 Stakeholders - Relationships, roles, and responsibilities of key players (e.g. user, supply chain, industry, etc.)

2. Program Performance/System Indicators & Requirements - Describes the key sustainment metrics. This section should include each metric along with its definition, objective, threshold and either its current projected value or its actual measured value.

2.1 Materiel Availability

2.2 Materiel Reliability

2.3 Mean Down Time

2.4 Ownership Cost

2.5 Additional key sustainment enabler metrics

3. Sustainment Implementation Plan

3.1. Supportability Design Characteristics - Describes the key requirements included in the system and design specifications.

3.2. Supportability Analysis Process - Describes the processes included in the Systems Engineering Plan being used to establish and keep the product support elements in balance in achieving the sustainment metrics.

3.3. Product Support Package - Describes the major product support elements and plan for

fielding the PSP meeting the outcome requirements within statutory and Component mandates.

3.4. Sustaining the Weapon System - Describes the systems engineering and management strategies to sustain the metrics including how ranges and triggers will be used.

4. Program Schedule - Shows how major sustainment actions/events fit with the overall program master schedule at the current funding levels.

5. Special Interest Items - Describes any additional information on key technologies, initiatives or enablers the program is using to implement the sustainment strategy and reduce total ownership costs the program wishes to highlight. (e.g. human systems integration (HSI), supply chain integration (including item unique identification (IUID)/radio frequency identification (RFID) technologies, diminishing manufacturing sources/materiel shortages (DMSMS), etc.)

Figure 5.1.2.2.F3. Notional Life-Cycle Sustainment Plan Focus Areas

LCSP Outline	Focus Area	MSA	TD	EMD	PD	O&S
Executive Summary						
1.0. Introduction						
2.0 Sustainment Concept	1.1	M	D	D	D	M
3.0 Sustainment Performance Requirements	2.0	M	D	D	D	D
4.0 Sustainment Acquisition Strategy	1.2		M	D	D	M
5.0 Sustainment Design Characteristics	3.1	M	D	D	D	M
6.0 Product Support Package Status Overview				M	D	D
7.0 Special Interest Items	5.0			M	M	M
8.0 Integrated Schedule	4.0		M	D	D	M
9.0 Funding and Costs	1.3		M	D	D	M
10.0 Management						
10.1 Organization	1.4		M	D	D	D
10.4 Sustainment Management	3.4		M	M	D	D
11.0 Supportability Analysis	3.2		M	D	D	M
12.0 Product Support Package Implementation	3.3			D	D	M
13.0 Other						
Phase Emphasis Code						

M = Major emphasis **D** = Major emphasis including program details						

Figure 5.1.2.2.F4. LCSP Outline With Focus Areas

Responsibilities. The Program Manager is responsible for the content and preparation of the LCSP. In developing and executing the LCSP, the PM should work with the user, the Product Support Manager, Product Support Integrator(s), and Product Support Providers to document performance and sustainment requirements specifying objective outcomes, resource commitments, and stakeholder responsibilities. Once developed, to help ensure an integrated team approach, the LCSP should be approved by the Program Manager, Product Support Manager, Contracting Officer, lead financial analyst and lead engineer.

5.1.2.3. Replaced System Sustainment Plan

Once a decision has been made that a system will replace another and it is required, the Service Secretary sponsoring the new Major Defense Acquisition Program (MDAP) (or the Commander of the United States Special Operations Command) shall prepare a Replaced System Sustainment Plan for the existing system. (10 USC 2437) It will include at a minimum the following which will require close coordination between any effected programs:

- The budget estimates required to sustain the existing system until the new system assumes the majority of mission responsibility. Consequently, it is critical that once a program is operational, its LCSP contain the current and required funding levels through the FYDP so that the additional funding through disposal can be easily added.
- The milestone schedule for developing and fielding the new system, including the scheduled dates for low-rate initial production, initial operational capability, full-rate production, full operational capability and the date of when the replaced system is scheduled to assume the majority of the mission responsibilities of the existing system.
- An analysis of the ability of the existing system to maintain mission capability against relevant threats including:
    - Anticipated funding levels necessary to ensure acceptable reliability and availability rates and maintain mission capability against the relevant threats.
    - The extent to which it is necessary and appropriate to transfer mature technologies from the new system or other systems to enhance the mission capability against relevant threats and provide interoperability with the new system during the period from initial fielding until the new system assumes the majority of responsibility for the existing system mission.

5.1.3. Life-Cycle Sustainment in the Integrated Product & Process Development (IPPD) Framework

5.1.3. Life-Cycle Sustainment in the Integrated Product & Process Development (IPPD) Framework

The IPPD is a management technique using multidisciplinary teams (Integrated Product Teams (IPTs)) to optimize design, manufacturing, maintenance, and logistics processes. The IPPD facilitates meeting cost, statutory, and performance objectives across the life cycle. It is a broad, interdisciplinary approach that includes not only the logisticians, engineers, technical specialists, contract specialists, and customers in the IPTs, but also business and financial analysts as well. (See also Guidebook sections 10.3, 11.8, and the IPPD Handbook.)

5.1.3.1. The Program Manager's Role in Life-Cycle Sustainment

The PM's responsibility is to provide the user with a sustainable system and product support that meets specified performance effectiveness and affordability requirements. PM's should continually measure, assess, and report program execution in terms of performance, schedule, sustainment, and cost outcomes. These efforts are critical both for establishing budgetary requirements and for tracking execution success over time for both new and legacy programs. The PM should reduce system downtimes and reduce Total Ownership Costs through deliberate use of systems engineering analysis during the design phase to design out the maintenance burden, reduce the supply chain, minimize mission impacts and reduce the logistics footprint.

In accomplishing this, the PM should examine and implement appropriate, innovative, alternative logistics support practices, including the best public sector and commercial practices and technology solutions. The choice of logistics support practices is based on the PM's documented assessment that they can satisfy users in a manner meeting statutory requirements that are fully interoperable within DoD's operational, logistics systems and enterprise; will improve schedules, performance, or support; or will reduce ownership costs. Regardless of the chosen support strategy, PMs should collaborate with other key stakeholders, especially the user, to refine and establish logistics support program goals for cost, customer support, and performance parameters over the program life cycle. The resultant decisions and planned actions are critical components in the Acquisition Strategy and the Acquisition Program Baseline.

An important performance-based life-cycle product support aspect is the concept of a negotiated agreement between the major stakeholders (e.g., the PM, the force provider(s)/users, and the support provider(s)) that formally documents the performance and support expectations and commensurate resources to achieve the desired outcomes. Per DoD Instruction 5000.02,

Enclosure 2, paragraph 8.c.(1)(d), "The PM shall work with the user to document performance and sustainment requirements in performance agreements specifying objective outcomes, measures, resource commitments, and stakeholder responsibilities." The term "performance agreements," as cited in DoD 5000-series policy, is an overarching term suitable for policy guidance. In actual implementation, the more specific term "performance-based agreements" is used to ensure clarity and consistency.

Demilitarization and Disposal: From the very beginning of a program, it is important that program managers consider and plan for the ultimate system demilitarization and disposal once it is no longer militarily useful. The PM should minimize DoD's liability due to information and technology security, and Environment, Safety, and Occupational Health issues. During the systems engineering process as the design requirements are established, the PM should carefully consider the life-cycle impact of any hazardous material component requirements to minimize the impact on the end item regarding item storage, packaging, handling, transportation, and disposition. (See section 4.4.5.)

5.1.3.2. Product Support Manager (PSM)

The day-to-day oversight and management of the product support functions are delegated to a product support manager (an overarching term characterizing the various DoD Component function titles, i.e. Assistant Program Manager for Logistics, Chief of Logistics, System Support Manager, etc) who leads the development and implementation of the performance-based product support strategy and ensures achievement of desired support outcomes. The product support manager, while remaining accountable for system performance, can delegate responsibility for delivering specific outcomes. In doing so, the PM and PSM may employ any number of sub system PSMs or product support integrators to integrate support from all support sources to achieve the performance outcomes specified in a performance-based agreement.

In accomplishing the outcomes, product support integrators (PSI) should have considerable flexibility and latitude in how the necessary support is provided. The activities coordinated can include functions provided by organic organizations, private sector providers, or a partnership between organic and private sector providers. While product support execution is accomplished by numerous organizational entities, the product support integrator is accountable for integrating all sources of support necessary to meet the agreed to support performance metrics as specified in a memorandum of agreement, memorandum of understanding, or contract as appropriate.

To effectively coordinate the work and business relationships necessary to satisfy the user agreement the product support integrator should be knowledgeable about the system, involved early in the program life, and incentivized to continuously improve reliability, maintainability, and sustainment technology. Candidates for the role include:

- A DoD Component organization or command.
- The system's original equipment manufacturer or prime contractor.
- A third party private sector logistics integrator.

Regardless of the approach taken, the government is ultimately accountable for delivering performance and warfighting capability to the user. Consequently the PSM is responsible for accomplishing the overall integration of product support either directly through government activities or via a contract when commercial organizations are involved. If any part of the product support strategy is contracted, a description of how it will be acquired should be documented in the Acquisition Strategy and LCSP.

5.1.3.3. Integrated Product Teams (IPTs)

The PM should establish multidisciplinary teams to develop and manage the implementation of the performance-based support strategy. The IPTs should consider all factors and criteria necessary to achieve an optimum support strategy using the best capabilities of the public and private sectors in a cost effective manner. DoD Component and DLA logistics activities should participate in support strategy development and IPTs to ensure the support concept is integrated with other logistics support and combat support functions and provide agile and robust combat capability. These participants can help to ensure effective integration of system oriented approaches with commodity oriented approaches (common support approaches), optimize support to users, and maximize total logistics system value.

The teams should be structured to provide a system orientation focused on the performance outcome instead of focusing on the individual logistics support elements or technical disciplines. The teams can consist of government and private sector functional experts; however, it is important they are able to work across organizational and functional boundaries. Consequently, representatives from DoD Component headquarters, operational commands, engineering, procurement, test, comptroller, information technology and logistics representatives from supply, maintenance, and transportation organizations should be considered for inclusion on the IPTs.

5.1.3.4. Stakeholders

Stakeholders consist of any group or organization with a related or subsequent responsibility that is directly related to the outcome of an action or result. Generally speaking they can influence the outcome or are the recipient of the results. The range of personnel selected to participate as stakeholders is based on the outcome and processes involved. Typical stakeholders are: users or operators, acquisition commands, test communities, depots, manpower, personnel & training communities, maintainers, and suppliers (e.g., DLA, the Inventory Control Point (ICP), US Transportation Command (TRANSCOM), industry, and other organizations associated with the sustainment chain).

5.1.4. Performance-Based Agreements (PBAs)

PBAs formally document the agreed to level of support and associated funding, required to meet performance requirements. The PBA with the user states the objectives that form the basis of the performance-based product support effort. They establish the negotiated baseline of performance

and corresponding support necessary to achieve that performance, whether provided by commercial or organic support providers. The PM negotiates the required level of support to achieve the user's desired performance at a cost consistent with available funding. Once the performance and cost are accepted by the stakeholders, the PM enters into PBAs with the user community which specify the level of support and performance. Likewise, PMs enter into performance-based agreements with organic sources and/or contracts with commercial sources which focus on supporting the users in terms of cost, schedule, and performance. Consequently, PBAs can describe agreements between 1) user and PM, 2) PM and support integrator(s), or 3) support integrator and support provider(s). The agreements should maintain flexibility to facilitate execution year funding and/or priority revisions and spell out the 1) objective outcomes, 2) performance measures, 3) resource commitments, and 4) stakeholder responsibilities. (See figure 5.1.4.F1.)

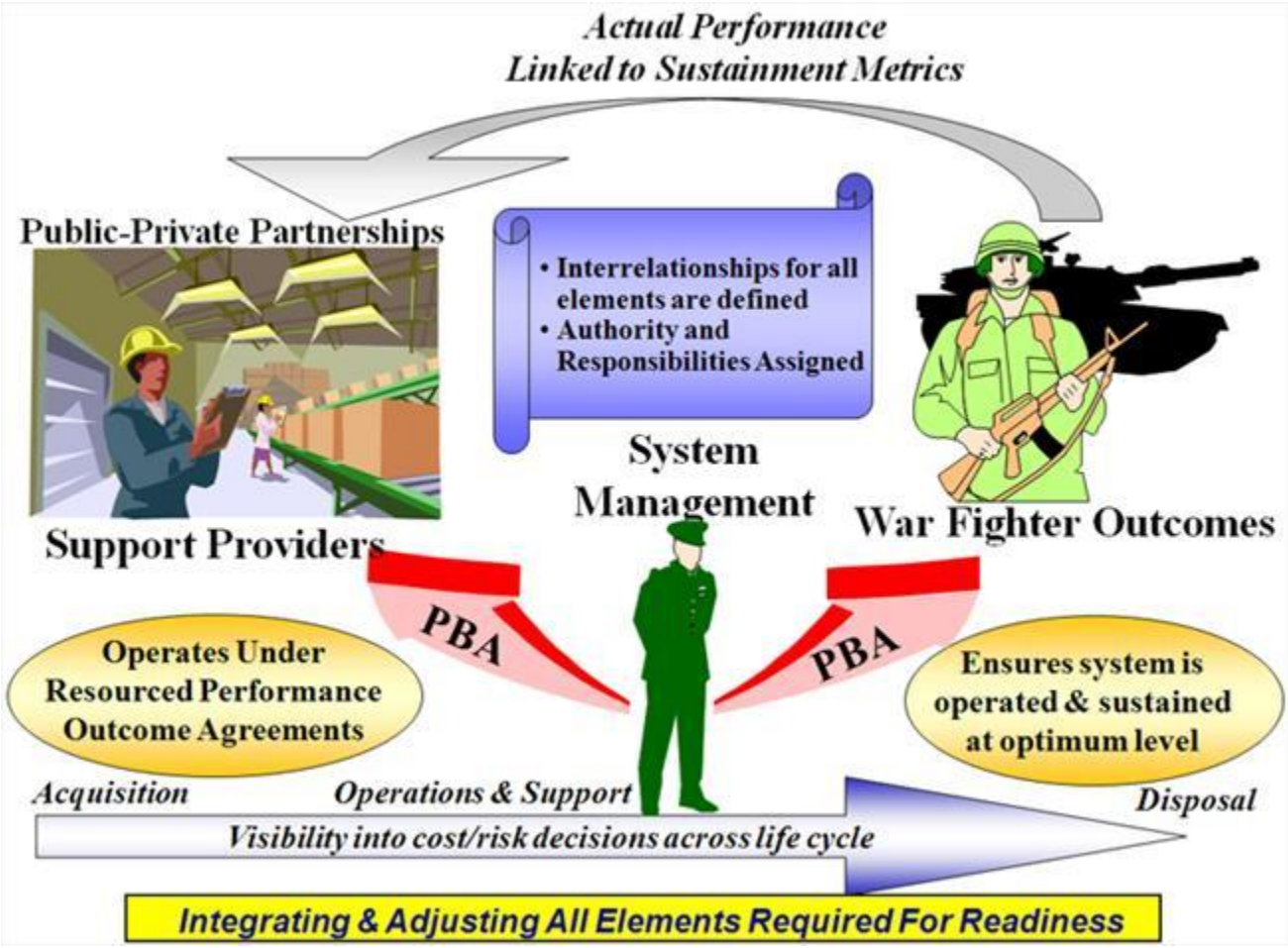


Figure 5.1.4.F1. Performance-Based Agreements

Sustainment metrics should provide the objectives that form the basis of the PBAs. The PBA performance metrics should reflect the highest level of metrics that are most critical in producing

the desired performance outcome(s). Generally, a focus on a few properly incentivized performance-based outcome metrics – such as materiel availability, materiel reliability, etc. – will lead to more effective solutions. However, in developing the agreements, it may not be possible to directly state these high level performance objectives as metrics due to lack of support provider control of the support activities necessary to produce the user performance (e.g., availability). This is because some DoD Component logistics policies and/or guidance mandate a preference for DoD Component performed maintenance and retail supply functions that cut across multiple organizations. Accordingly, the PM may select the next echelon of metrics for which the support provider can be held accountable and which most directly contribute to the sustainment metrics.

The outcome metric to achieve the user requirements (e.g., materiel availability) should be a balance between a quality metric (e.g., materiel reliability), a response metric (e.g., turn around time), and a cost metric that are appropriate for the outcome needed. Many existing logistics and financial metrics can be related to top level user performance outcomes. These include, but are not limited to, logistics footprint, not mission capable supply (NMCS), ratio of supply chain costs to sales, maintenance repair turnaround time, depot cycle time, and negotiated time definite delivery. In structuring the metrics and evaluating performance, it is important to clearly delineate any factors that could affect performance, but are outside the control of the support providers.

While objective metrics form the bulk of the evaluation of a provider's performance, some elements of product support might be more appropriately evaluated subjectively by the user and the PM team. This approach allows some flexibility for adjusting to potential support contingencies. For example, there may be different customer priorities to be balanced with overall objective measures of performance.

Agreements with Organic Providers: Organic providers, like commercial providers, will have a set of performance metrics that will be monitored, assessed, incentivized, and focused on the system. For support provided by organic organizations a performance-based agreement, similar in structure to a memorandum of agreement, memorandum of understanding, or service level agreement, may be used to represent and document the terms of the agreement for organic support. One important distinction, however, between PBAs and other types of agreements and understandings is that PBAs contain the agreed to performance and/or sustainment metrics meeting the user requirements tied to funding.

5.1.5. Contracting for Sustainment

5.1.5. Contracting for Sustainment

For support provided by commercial organizations, the contract is the PBA reflecting the agreed to user performance requirements. (Source of support decisions do not favor either organic or commercial providers. Non-core source of support decisions should optimize the best public and private sector competencies based on a best value determination of the provider's capability to meet set performance objectives.) The major shift in the environment from the traditional approach is how programs acquire support, not from whom it is obtained. Implementing a performance-based acquisition and sustainment strategy begins with integration into the systems engineering process to establish the right performance metrics. This is because instead of buying set levels or varying quantities of spares, repairs, tools, and data, the focus is on designing in sustainment features and buying a predetermined level of readiness to meet the user's objectives. (See section 11.6, Implementing a Performance-Based Business Environment.)

5.1.5.1. Contract Characteristics

The preferred contracting approach is the use of long term firm fixed price contracts with incentives tied to outcome performance to fulfill the product support and integrated sustainment chain management responsibilities. Consequently, the contract should provide support over a specific period of time for a predetermined fixed cost per operating measure. Sustainment contracts should require the delivery of a capability to the user using a Statements of Objectives or a Performance Work Statement approach. (Level of effort or labor hour type contracts are not preferred because they limit the contractor's ability to make necessary trade-offs to meet and/or exceed the threshold performance outcomes within the funding profile.)

A sustainment contract may take many forms and the degree to which the outcome is defined varies. It should purchase support as an integrated performance package designed to optimize system readiness. It must specify performance requirements; clearly delineate roles and responsibilities on both sides; specify metrics and their definitions; include appropriate incentives; and specify how performance will be assessed. The contract should cover the procurement of a capability to support the user versus the individual parts or repair actions and provide the ability to manage support providers.

Award term contracts should be used where possible to incentivize industry to provide optimal support. Incentives should be tied to metrics tailored to reflect the DoD Component's specific definitions and reporting processes. Award and incentive contracts should include tailored cost reporting to enable appropriate contract management and to facilitate future cost estimating and price analysis. Sustainment contracts should strive to specify a fixed cost per outcome (e.g., operating hour (e.g., hour, mile, cycle) or event (e.g., launch)) vice a cost plus contract. However, lack of data on systems performance or maintenance costs or other pricing risk factors may necessitate cost type contracts until sufficient data is collected to understand the risks. Full access to DoD demand data should be incorporated into any contracts. The contracts should be competitively sourced wherever possible and should make maximum use of small and disadvantaged businesses.

Contracts must follow Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) guidance, as appropriate, for the acquisition of logistics services and support throughout the program life cycle. In addition, competition over the entire life cycle can be a valuable tool for achieving affordable sustainment. Consequently, early in the program, the PM should consider the cost versus benefit of the data and other support elements required to achieve competitive versus sole source contracting for sustainment functions (e.g. parts, repairs and other supply chain processes).

5.1.5.2. Methodology for Implementing Sustainment Contracts

The contracting methodology is a multiple step process that can be applied to new, modified, or legacy systems at the system, subsystem, or major assembly level covering a range of functions depending on program unique circumstances. Additional guidance is contained at https://acc.dau.mil/pbl but the steps can be summarized in the following general areas:

Define the Requirements: The initial step is to relate or determine the performance outcome metric meeting the user's needs rather than to rely on discrete transactional logistics functions. Care should be given to ensure the costs and performance metrics selected focus measurable contractor behavior in terms of the metrics selected. Defining and documenting the requirement involves answering three key questions: Who are the key stakeholders? What are the operations and sustainment environment and infrastructure? What are the total system cost and performance objectives? To develop an effective contracting strategy, the PM needs to identify the risks and benefits to achieve the desired outcome. Evolving system sustainment requirements should be constantly equated to long term financial resources.

In determining the extent to which contracts will be used, the PM should determine the best mix of public and private sector capabilities to meet evolving user requirements, joint sustainment opportunities, and the statutory requirements. (DoD Directive 5000.01, E1.1.17) This involves identifying the best mix in terms of: capability, skills, infrastructure, opportunities for partnering, compliance with Title 10, public/private flexibility, and affordability for each support function. As operating scenarios and technologies change, supportability related performance requirements may change. Thus, refining and resources for system requirements is a continual management process.

Sustainment contracts should produce measurable performance outcomes that cumulatively contribute to the sustainment of system KPP/KSAs, to their threshold or objective levels. To motivate the contractor to achieve the desired behavior, appropriate contract incentives (including award fee, incentive fee, award term, and cost sharing) need to be developed to promote and facilitate contractor performance.

Develop and Award the Contract: From a sustainment perspective, contracts should be structured to balance three major objectives throughout the life cycle of the system: 1) delivering sustained materiel readiness; 2) minimizing the requirement for logistics support through technology insertion and refreshment; and 3) continually improving the cost-effectiveness of

logistics products and services. Careful balancing of investments in logistics and technology to leverage technological advances through the insertion of mature technology is critical. In addition, the PM should insure the contract addresses user requirements during peacetime, contingency operations, and war and provides for the capability for the government to compete or take over the sustainment responsibility in the future.

Contract development is a lengthy, complex process, led by the PM, involving multiple stakeholders. No two contracts are exactly the same – each must be tailored to the unique requirements of the system considering, at minimum, the factors and criteria listed below:

- **Statutory requirements:** Title 10 U.S.C. 2460, 2464, 2466, 2469, and 2474 (Core, 50/50, public/private partnering, etc.). Depot maintenance partnerships can be effective tools to implement performance-based product support arrangements if properly structured. The contracts should allow partnering with public depot maintenance activities to satisfy the requirements. (Examples and further discussion of public private partnerships can be found on the Acquisition Community Connection web site.)
- **Regulatory requirements:** DoD (e.g., DFARS) and DoD Component policy (including contractors on the battlefield, service performance of organizational level support functions, etc.).
- **Financial Enablers:** Ensuring the financial enablers are commensurate with the risks.

Implement and Assess Performance: The life-cycle management concept includes assessing actual system performance, readiness, and ownership costs and then revising the sustainment strategy and contracts as necessary. During contract execution, the program manager also acts as the user's agent to certify performance and approve incentive payments. Since no contract/agreement is self-regulated, the PM must accurately capture, analyze, and report sustainment related performance and cost data. PMs should periodically validate the contract business case with actual cost and performance data to ascertain if projected returns on investments are being attained and whether the basic support strategy still save the government money and should be continued.

5.1.6. Data, Software, and Intellectual Property Rights

5.1.6. Data, Software, and Intellectual Property Rights

Under the life-cycle management concept, the program manager must ensure that all data and software required to successfully procure and sustain the system is available throughout its life cycle, ensuring that competitive sourcing is considered. (See section 4.2.3.1.7 for additional data management information.) This includes product definition, materials, and parts information; product operational information; software; and associated information needed to competitively sustain throughout the life cycle. There are a number of statutory and regulatory definitions and procedures governing these subjects, and this chapter will not attempt to capture every detail or to replace the need for expert contracting and legal advice; but an overall understanding of the most common situations is important. The two major categories defined by statute are "Technical Data" and "Computer Software," each of which is governed by specific and slightly different regulations. "Computer Software Documentation" is a unique category that is included in the statutory definition of Technical data, and also is included under the rights of the Computer Software to which it pertains. Throughout this chapter, the specific terms will only be used when there is a critical distinction to be made, otherwise reference will be made generically to "data." Technical data does not include project or administrative types of information (e.g., financial, schedules, plans, and cost information) or transactional data. Any data products that do not fall within the statutory definitions exist in an undefined category are referred to as "Management Data" in the following discussion. See figure 5.1.6.F1 for a list of major data categories.

- **Technical data** includes recorded information, regardless of the form or method of the recording, of a scientific or technical nature. It includes:
    - Product Data includes the data created as a consequence of defining (requirements), designing (including the engineering drawings), testing, producing, packaging, storing, distributing, operating, maintaining, modifying and disposing of a product.
    - Computer software documentation including owner's manuals, user's manuals, installation instructions, operating instructions, and other similar items that explain the capabilities of the computer software or provide instructions for using the software.
    - Computer data bases (e.g., a collection of data recorded in a form capable of being processed by a computer) is treated as technical data based on the nature of the data contained in the data base.
- **Computer software,** including computer programs, source code, source code listings, object code listings, design details, algorithms, processes, flow charts, formulae, and related material that would enable the software to be reproduced, recreated, or recompiled.
- **Management data** includes data incidental to contract administration such as financial and/or management information, including most

cost, schedule, and other significant management deliverables. (Note the licensing and marking requirements established for technical data and computer software do not apply to management data.)

- **Source selection data** and contractor data submitted in support of a proposal have unique status and procedures and are not generally considered technical data.

Figure 5.1.6.F1 Major Data Categories

5.1.6.1. Data and Software Concepts

The key to success is ensuring requirements and strategies are identified and acted on early in the acquisition to avoid unexpected costs to procure, reformat, or deliver data. Important basic principles are summarized below, but programs are encouraged to refer to the cited references for full details and consult with contracting and legal subject matter experts for further assistance.

- Data deliverables or data items are delivered in response to contract requirements for data that has a pre-determined content and format. There is generally no automatic delivery of data, nor does the government have any automatic rights to technical data. To receive data or have access to data the government must explicitly require it under a contract using a Contract Data Requirements List (CDRL). In general, the contractor continues to own the actual data or intellectual property; government owns the deliverable and has license rights that govern how the data may be used.
- Computer Software generally is procured as one or more deliverable items (configuration items) identified in a contract rather than as Data under CDRL. Computer Software Documentation should be identified in the CDRL with the other items of technical data.
- The government's license rights (or data rights) are determined, in most cases, by the source of the funding used to develop the actual item (hardware or software) to which the technical data pertains. This is important when items are acquired as commercial items because there are unique regulations and contract clauses that apply to the acquisition of commercial items and commercial software. This must be considered even when the systems are not acquired as commercial items because subsystems or components within the major system may be acquired as commercial items.
- Contractors who own intellectual property have the burden of managing and protecting their rights. Unless a contractor asserts restrictions or limitations on the government's rights in technical data ordered under a contract, the government is entitled to unlimited rights to the data. In general, the government may not require contractors to sell or relinquish any rights in data they legitimately hold as a condition of doing business with the government, nor can the use of such data be discouraged. However, regulations do list

a number of data types that must be provided with unlimited license rights to do business with the government including:

- Studies, analyses, test data, etc. developed under the contract when the study, analysis, or test was specified as an element of performance
- Form, fit, and function data
- Data necessary for installation, operation, maintenance, or training purposes (other than detailed manufacturing or process data)
- Data to which the government has acquired license rights by other means.

It is critical the program understands these concepts to structure the contract data requirements and a data management approach that fulfills the government's needs, while protecting industry's intellectual rights.

Rights in Technical Data (Technical Data Rights) and Rights in Computer Software: In most cases, while the government owns the delivered physical medium on which delivered data resides, ownership of the data (the intellectual property) remains with the developer, even if the government has funded 100% of the development. The government receives license rights that determine how the data may be used. Unless a contractor has a legitimate basis to limit the government's rights, all data deliverables must be provided with unlimited license rights.

Unlimited rights means the right to use, modify, reproduce, perform, display, release, or disclose technical data in any manner, and for any purpose whatsoever, and to have or authorize others to do so. The government may freely use or disclose the data for any purpose whatsoever (absent any separate classification, distribution, or International Traffic in Arms Regulations (ITAR) restrictions).

If a contractor has funded the development of an item completely at private expense, then he may limit the government's use of technical data using limited license rights, or restrict the government's use using restricted license rights.

- **Limited rights** means the government may use the data within the government but not release the technical data outside of the government (not even to support contractors), except if necessary for emergency repair or overhaul, and may not use the data for manufacturing additional quantities of the item.
- **Restricted rights** means the government may only run the software on one computer at a time, may make only the minimum copies needed for backup, but may make modifications to the software. The software may not be released outside of the government except for emergency repair or overhaul.

Limited and restricted rights data must be closely guarded by government personnel to prevent unauthorized disclosure.

Frequently, both government and private funds are used in development efforts. In these cases, the contractor may be entitled to offer technical data or computer software with **Government**

Purpose Rights (GPR). GPR is essentially a middle path unique to defense contracts that offers a way for contractors to exploit intellectual property commercially for a limited period of time while the government also gets immediate benefits. GPR expires after a time limit (the standard is five years), at which point the government receives unlimited license rights. During the time, the government must limit the disclosure of the data outside of the government to government purposes. The government may release GPR data as part of a competition, but the data may not be used for commercial purposes. Generally, any disclosure of GPR data must be done using non-disclosure agreements to protect the developer's rights and to ensure the government is protected from inadvertently disclosing data.

The last category is **Specifically Negotiated License Rights (SNLR)**. This category pertains whenever the standard license arrangements are modified to the mutual agreement of the contractor and the government. In this case, the exact terms are spelled out in a specific license agreement unique to each application.

If the government needs to use data for purposes that are not supported by the license rights identified by a contractor, the additional rights must generally be negotiated for and will generally carry additional cost if the contractor is willing to sell at all. As a best practice, this should be done during the RFP process.

5.1.6.2. Data and Software Requirements and the Contractor's Assertions Lists

While the overall topic of data rights and intellectual property is complex, the statutes and regulations have created a relatively straightforward process for programs. The key to resolving or avoiding data problems is early and unambiguous identification of the government's data requirements. None of the statutes, regulations, or policies requires any specific data to be delivered, and the entire rights in data process only comes into play once a data deliverable has been required. Data identification is the most important step in the entire process and it drives the approach for acquiring and managing the data.

Having established data needs and developed a corresponding data strategy, the data deliverables must be established as requirements in the RFP. The required DFARS clauses will be incorporated into the RFP by the contracting officer. A best practice is to take the additional step to clearly identify which of the data categories each deliverable falls within. Many issues can be avoided simply by clarifying which category of data is intended in each CDRL, based on the categories established in the regulations. For example, CDRLs could clearly be broken into the categories of technical data, computer software documentation, and management data. Computer Software can be identified as specific contract line items to be delivered. Further, specific CDRL items intended to convey form, fit, and function data or that are intended to provide operating, maintenance and training data (such as technical manuals) should identified as such. In this way, there should be no misunderstanding that these items fall under the category that must be delivered with unlimited license rights.

Once the government has issued the RFP, the burden falls to the contractor(s) to respond properly in their proposals, to identify and mark deliverables, and to protect and manage their intellectual property properly. The contractor must identify any deliverables that will be provided with, other than unlimited license rights in what is referred to as an Assertions List, and must provide the basis for making these assertions. This includes deliverables at all levels in the contractor, subcontractor, and supplier hierarchy. There are strict limitations on the contractor's ability to add items to this list following contract award, so responsible prime contractors take great pains to thoroughly review these requirements with suppliers. (Generally, the only legitimate basis for asserting other than unlimited license rights is that the development of the actual item the technical data describes was done at private expense.) A specific format and required contents for the assertions list for Technical data is provided in DFARS 227.7103-10.

The only way contractors can protect data is by correctly listing it on the assertions list and correctly marking the deliverables in accordance with the DFARS. The requirements for marking data by the contractor are very specific and must be observed precisely. If these requirements are not met, the markings may not have to be observed by the government. It is the contractor's responsibility to ensure that only data legitimately qualifying is marked as limited, restricted, or GPLR data, and to ensure any markings are in the correct form and format. There is no DFARS provision for contractors, after contract award, to withhold data deliverables required by contract by asserting they are proprietary. The only mechanism is to list such items on the assertions list and then properly mark in accordance with the DFARS when submitted. After the fact assertions by subcontractors that data is proprietary or will be provided with other than unlimited rights should not be automatically accepted by the government.

Management data presents a unique challenge, as the rules are not quite so explicit. A best practice is for PMs and contracting officers to establish clear agreements with the contractor on what management data items require some form of special handling by the government based on their containing cost, pricing, process, or other data that warrants special handling but that does not fall under the rules set out for technical data. Such agreements might spell out the specific data involved, the markings to be used, and the protection and disclosure details agreed to. Such agreements facilitate data management and avoid confusing management data with technical data and potential misuse of the technical data markings or legends.

Data Markings, Reviews, and Challenges: Contractors are responsible for maintaining processes and procedures to ensure their intellectual property is protected, and for maintaining records to support any assertions of rights in data. The government is not automatically bound by contractor assertions or data markings, and all deliverables should be reviewed for unjustified or non-conforming markings (see 227.7103-12 for additional detail). The government may question or challenge the inclusion of items on the contractor's assertions list before or after contract award in accordance with DFARS procedures (see 227.7103-13 for additional detail). While contracting officers are responsible for the formal challenge process, the program needs to be able to identify data marking issues for potential action. Highlights for questioning or challenging markings are summarized below.

Justified vs. Unjustified markings: All deliverables should be reviewed against the Data Assertions List to ascertain whether each deliverable is marked in accordance with the contractor's assertions. Any differences should be identified, either as data that appear to bear an unjustified marking, or as data on the assertions list but has been submitted without the specified markings. Generally, contractors are provided the opportunity to correct markings before formal action is taken. The contractor bears the responsibility to mark data items if they want to protect their intellectual property rights, and the government does not have the responsibility to protect data items that are not marked. Similarly, data items bearing unjustified markings should be corrected, but ultimately the government is not obligated to protect data items that carry unjustified markings.

Programs should be vigilant in questioning the widespread use of legends, such as proprietary or competition sensitive, unless these terms have specifically been included in agreements related to management data.

Conforming vs. Non-conforming markings: DFARS 252.227-7103 contains specific requirements for marking data subject to limited, restricted, government purpose, or Specifically Negotiated License Rights. These requirements must be adhered to without exception for the marking to be valid. The program should ensure the process of reviewing data deliverables includes a review of justified restrictive markings for conformance to the DFARS requirements. The contractor generally is given an opportunity to correct non-conforming markings; but in the long run, the government is not obligated to respect or protect non-conforming markings even if the data item is otherwise entitled to protection.

Programs should be vigilant in ensuring only the portions of data deliverables containing data subject to limitation or restriction is marked. Frequently, entire documents are marked on every page while only portions of selected pages contain the actual data subject to the limitation or restriction. Only the specific pages or portions of pages should be marked with the legend. Unless corrected at the earliest opportunity, data marked with unjustified or inappropriate legends will generally be treated as if the markings were correct, potentially adding unnecessary cost for controlling the data and in some cases limiting opportunities for competition.

5.1.6.3. Contracting for Technical Data

Program Managers should consider, when cost effective, the acquisition of complete technical data packages to ensure compeititon, or the option of competition, at both the prime and subcontractor level throughout the life cycle. The DFARS provides two standard clauses frequently used as part of the data management strategy. **Deferred delivery** allows for the actual delivery of certain pre-determined CDRL items to be deferred until two years after the acceptance of all other items under the contract. **Deferred ordering** allows the government to order the delivery of any technical data or computer software generated under a contract until three years after the acceptance of all other items under the contract. Realistically, deferred delivery is beneficial in limited instances where the government defers the cost of storing or maintaining data for some period of time, perhaps to better determine whether there is a real

need to hold that data within the government. Deferred ordering is not a remedy for poor data planning and will not solve all long term data problems. To order the deferred delivery, the data must have been actually developed under the existing contract. A common practice in recent contracts has been the requirement for contractors to develop a Data Accession List as a CDRL item. The Data Accession List requirement specifies particular types of data that must be catalogued and retained by the contractor if they are developed in the course of contract execution but are not otherwise deliverable to the government. This Data Accession List then becomes a catalogue for ordering under the deferred ordering clause. Potential issues relating to license rights are best avoided by making government requirements clear and unambiguous so any limitations or restrictions may be addressed in the contractor's initial assertions list. Deferred ordering does not allow the ordering of new data items that have not already been created, nor does it allow the ordering of data items developed under other contracts or with private funding.

Program managers and contracting officers have great flexibility to create unique solutions to best suit program needs under current laws and regulations. One of the approaches, the use of **priced option agreements** to purchase data or additional license rights, must be addressed in the data strategy per statute and policy. As part of the data management strategy, the program manager must assess the merits of including priced option agreements for the purchase of additional data or additional license rights not initially acquired. This approach requires that in addition to the data required by the DFARS clause for the assertions list, contractors provide a priced option to acquire license rights beyond those contained in the basic bid. For example, a subsystem supplier may have developed a subsystem entirely at private expense, and therefore will provide detailed drawings with limited data rights. The PM may reasonably believe the government will need to develop a second source for this subsystem and may request the contractor identify the price to acquire GPLR or unlimited rights in the drawings. The contractor is not obligated to respond, but may choose to identify a price for the additional license rights. The key to this approach is that the data items (content and format) must be identified as specifically as possible.

Another approach is to use options for the future acquisition of such data or license rights. This approach may be applicable in cases involving technology which is very valuable to the developer today, but is subject to rapid obsolescence. In some cases, the cost to acquire data or license rights today is prohibitive, but the owner may be willing to offer an option to buy in the future at a much lower cost. **Data escrow** is frequently used in the software industry. Generally, the developer delivers a copy of the relevant deliverable to a neutral third party for safekeeping during a predefined escrow period. Within the escrow period, the government may obtain delivery of the item if certain conditions occur. The parties must negotiate a number of important elements, such as the escrow period, the conditions under which the government can require delivery, the procedures for requesting delivery, and the payment of escrow fees.

5.1.6.4. Data Management Strategy

DFARS requires major programs to develop a long-term strategy integrating data requirements across all functional disciplines, to include logistics. While the title is "Data Management

Strategy," the content should include the approach to managing intellectual property issues relating to any computer software as well. The Data Management Strategy must be part of the Acquisition Strategy for major systems and is a best practice for all acquisitions. It must contain at least the content specified by statute (10 USC 2320 and Public Law 109-364) and regulation (DFARS part 227 and DoD Instruction 5000.02, Enclosure 4, Table 2-1, and Enclosure 12, paragraph 9.a) including:

- Assessing the data required to design, manufacture, and sustain the system as well as to support re-competition for production, sustainment, or upgrades.
- Addressing the merits of including a priced contract option for the future delivery of technical data and intellectual property rights not acquired upon initial contract award.
- Considering the contractor's responsibility to verify any assertion of restricted use and release of data.

The Data Management Strategy should describe the measures taken to acquire complete technical data packages to ensure competition. This should include describing the disciplined processes and systems that will be used to plan for, acquire, and/or access, manage, and use data throughout the life cycle, concentrating on technical and logistics data in support of the development, production, operation, support, improvement, demilitarization, and disposal of the system. (Also see section 4.2.3.1.7 for a discussion of data management in systems engineering.) It should address all forms of recorded information, regardless of the method of recording, and include both government and contractor-created data. The strategy should describe the program's approach and process of applying / implementing data management policies, systems, and procedures for:

- The analysis of data use to identify the data requirements
- The timely and economical acquisition of the data
- Assuring data adequacy and accuracy
- Data access, distribution, or communication to the point of use

The Data Management Strategy must be approved and integrated with the Acquisition Strategy prior to issuing a contract solicitation and should specifically address the:

- Data required to cost effectively operate, maintain, and improve the fielded system as well as foster competition throughout the system life cycle.
- Government rights to the data acquired, including the requirements for delivery or access. For example, to support DMSMS screening, access to the indentured bill of materials (BOM), showing the relationships of parts, components, assemblies, etc. is frequently required, even when rights to make further use of the BOM data may not be.
- Approach for ensuring data is available in a format compatible with the intended user's environment. Each program tailors the data strategy to the unique needs of the program, however, whenever data is delivered to the government, it should be formatted in accordance with accepted data standards to ensure usability by the government. A list of data standard examples can be found in section 4.2.3.1.7.

- Quality assurance program to guarantee the accuracy and completeness of the data.
- System for managing the data requirements and data.

See figure 5.1.6.4.F1 for a notional outline of one way in which the strategy can be documented.

---

1. **Data needs.** This section should summarize how long term needs for data were assessed, including data needed to support subsystems and components of the total system. This assessment should consider the needs of the entire life cycle, extending through operations to disposal. Potential competition/re-competition for procurement of the system, subsystems, components, logistics support including spare and repair parts should be included.
2. **Data acquisition strategy to be employed.** This section should describe:
    a. The data deliverables specified in the RFP or contract, including the technical data, computer software documentation, and management data items.
    b. The degree to which data will be acquired to support future competitions. It should include the logic by which these elements were selected; the alternative solutions considered; and the criteria by which the decision to procure technical data was made.
    c. The extent priced options to acquire additional license rights will be used.
    d. The intended use of other mechanisms such as deferred ordering, deferred delivery, and the use of withholding or incentives specific to performance in the area of data management.
    e. How the use of an integrated digital environment and the repository system factors into the data strategy.
    f. The digital format standards to be used and why they were selected. The process (i.e., business case analysis, adherence to DoD Component policy, etc.) used to determine the deliverable form/format for all deliverables should be included.
3. **Data management approach.** This section should describe how data will be managed throughout the system life cycle including:

    a. Data management responsibilities within the program.
    b. The overall approach to managing data acquired with other than unlimited rights.
    c. How the data deliverables will be reviewed for unjustified or non-conforming markings. It should include the process the program will follow to question or challenge contractor assertions or markings.
    d. The management approach for management data (i.e. data that is not software or technical data). It should include how contractor data meeting protection will be identified, marked, and managed.
    e. Any required interfaces to government data systems or repositories, and how those requirements will be satisfied.

f. The approach for maintaining the software and its documentation once software maintenance is transferred from the OEM. It should include the contract provisions being put into place that will allow for a cost effective migration.

Figure 5.1.6.4.F1. Notional Data Management Strategy outline

5.1.6.5. Data Management System

The Data Management Strategy should be supported by an integrated system that meets the needs of both the user and the support community. Data systems supporting the total life cycle should be connected, real-time or near real-time, to allow logisticians to address the overall effectiveness of the logistics process in contributing to system availability and life-cycle cost factors. Melding acquisition and sustainment data systems into a true total life-cycle integrated data environment (IDE) provides the capability needed to reduce the logistics footprint and plan effectively for sustainment, while also insuring that acquisition planners have accurate information about life-cycle costs. Using concepts contained in section 7.4, an integrated data management system:

- Facilitates technology insertion for affordability improvements during re-procurement and post-production support;
- Supports configuration management processes;
- Enables maintenance and supportability analyses; and
- Supports contract service risk assessments over the life of the system.

The ideal solution for government access to manufacturing, repair, and maintenance records is the establishment of a cost effective industry standards based process for the storage, access, and analysis of such data. Such a process should provide the PM and the user with immediate, worldwide access to the authoritative source of information required for manufacture, servicing, and maintenance/repair. The process should have the capability to capture original, unaltered documentation/data and to maintain the documentation/data for the entire system life cycle. There are many ways a program can elect to implement data management concepts and the plan should describe the program's approach for addressing the above factors. For example: mission critical government acquired data could be maintained in an industry standardized, Web-based repository with government access. In other cases, leaving government acquired data in the physical possession of the contractor and having access to the contractor's data system is the best solution. Regardless of the path chosen, the strategy must consider the life-cycle data implications through disposal.

Maintaining data in an IDE does not automatically resolve all data and license rights issues, and may add complexity to the management of license rights. For example, there is a substantial difference between requiring that a contractor provide access to view data on a contractor's system to requiring that data be delivered in place and stored on the contractor's system for

subsequent delivery to the government. The Data Management Strategy should discuss the IDE approach and how the program is managing data and supporting data systems in support of long term program needs.

Data Protection. Whether data are stored or managed by government or by industry, the PM is responsible for protecting system data. (See section 4.2.3.1.7.2) Program managers must ensure program data is protected in accordance with classification requirements. In addition, distribution and marking of program data must be managed in accordance with ITAR regulations, Freedom of Information Act and Privacy regulations, and federal requirements for record retention and management. When the data is not within the PM's direct control it should be marked so that the data management systems can ensure only authorized users have data access. Policy applicable to data protection, marking, and release can be found in the following publications:

- DoD Directive 5230.24, Distribution Statements on Technical Documents;
- DoD Directive 5230.25, Withholding of Unclassified Technical Data From Public Disclosure;
- DoD Instruction 8500.2, Information Assurance (IA) Implementation;
- DoD 5400.7-R, DoD Freedom of Information Act Program; and
- Defense Federal Acquisition Regulations Supplement (DFARS) Part 252.227-7013 & 7014.

5.1.6.6. Additional Technical Data Information

Data management in defense acquisition programs is governed by a complex mix of statutory and regulatory requirements developed over decades in an ongoing effort to balance the government's needs and the legitimate interests of developers of intellectual property. Primary references in addition to DoDI 5000.02 are FAR part 27 and DFARS part 227 as well as the OSD AT&L guide, Intellectual Property: Navigating Through Commercial Waters, Issues and Solutions When Negotiating Intellectual Property With Commercial Companies. DoDI 5010.12-M, Procedures for the Acquisition and Management of Technical Data, also contains useful descriptions of basic data management practices.

Industry standards organizations such as Information Technology Association of America/ Government Electronics and Information Technology Association (ITAA/GEIA), International Organization for Standardization (ISO), and American National Standards Institute (ANSI) provide high level principles to guide integrated data management planning, and implementation. GEIA Standard 927, Common Data Schema for Complex Systems, GEIA-STD-0007, Logistics Product Data, EIA-836A, Configuration Management Data Exchange and Interoperability and GEIA-859, Data Management (which are available for purchase) may be helpful for PMs and data managers. The standard and the handbook outline principles and processes for the management of data including data interoperability and longevity, best practices, and long term electronic storage, use, and recovery of data.

5.1.7. Configuration Management

Program Managers establish and maintain a configuration control program, and are required to "base configuration management decisions on factors that best support implementing performance-based strategies throughout the product life cycle" (DoD Directive 5000.01). An effective configuration management program should include configuration control over the functional and allocated baselines as well as the physical baseline. The approach and responsibility for maintaining configuration control will depend on a number of program specific factors such as design rights, design responsibility, support concept, and associated costs and risk. Nominally the government maintains configuration control of the system design specification and retains the authority/responsibility for approving design changes impacting the system's ability to meet specification requirements. The contractor(s) has the right to access configuration data at any level required to implement planned or potential design changes and support options.

Section 4.2.3.1.6 provides additional configuration management (CM) information including useful references. In addition, the ANSI/EIA-649 National Consensus Standard for CM and corresponding handbook are key joint government/industry developed documents intended to give guidance on the development and execution of a Configuration Management Plan. These configuration management discussions generally apply to legacy programs with traditional CM programs; however, the use of performance-based product support contracts and public private partnerships necessitate DoD logisticians understand, apply and address the CM impacts as they implement the sustainment strategy. This is because if the configuration of the system is not monitored closely, design control could be lost, resulting in procuring a useless product support package. This would make it difficult to provision or ensure the proper support equipment, spares, and data are available to complete repairs, thereby adversely affecting materiel availability and increasing program costs.

The logistician's involvement in the configuration management process is vital throughout the system's life cycle. The logistics process enters into the configuration management world through support and maintenance planning, since the maintenance plan drives the level of government configuration control and support element requirements. During the maintenance planning process, factors such as reliability and volatility of the design technology are used to determine how the system/component will be supported, e.g., throwaway or repair, and commercial or organic repair.

In commercial support strategies, it is not uncommon to delegate broad Class II (no change in form, fit, function, or testability of an item) configuration management to the product support provider. Since the provider is tasked to deliver performance outcomes with broad flexibility regarding how to provide those outcomes, it is consistent to also provide him flexibility to implement configuration changes (with government knowledge) stemming from his investments to improve reliability, availability, and repair processes that benefit both the government in terms of improved readiness and the commercial provider in terms of profit opportunities by reducing cost over the contract term.

Also, in PBL contracts, provisions should be made to protect the government in the event the contractor is unable to provide the contracted performance and at contract conclusion. Technical Data is an important component of the configuration management process so it is vital the PM understand the level of access to technical data packages (TDP) required to successfully procure, compete, and sustain the system over its entire life cycle. This level will vary from system to system and often down to the component or part level. Specific clauses must be included in the contract to ensure the government retains access to or takes control of the necessary TDP(s) and corresponding TDP updates. This ensures the government will have the data necessary to duplicate the existing configuration with little to no interruption in the support provided to the user if the support provider changes or the contract is re-competed. Without this exit ramp, the government will not be able to cost effectively re-compete a system and/or component.

5.2. Applying Systems Engineering to Life-Cycle Sustainment

Figure 5.2.F1 depicts the Life-Cycle Management System and relates key sustainment design and systems engineering activities. (Figure 5.2.F1 provides an overview roadmap during the acquisition process. Expanded versions are shown by phase in section 5.4.) These system engineering processes are not carried out in a strictly linear progression; they are typically carried out iteratively, expanding into lower levels of detail as the design evolves. Incremental acquisition present challenges in both acquisition and sustainment activities. An obvious challenge is the potential cost and configuration management challenges that can arise with multiple configurations of end items as well as the support system. This should be addressed early in development and evolution of the acquisition strategy. If planned correctly, configuration management efforts combined with rapid prototypes can provide the PM the opportunity to observe and evolve the success of tentative support strategies. Conversely, poor management of multiple system configurations can create a significant sustainment burden.

Program teams manage programs "through the application of a systems engineering approach that optimizes total system performance and minimizes total ownership costs" (DoD Directive 5000.01). In doing so, the PM's overriding program objective should be to maximize system effectiveness from the user's perspective. To accomplish this, sustainment considerations are addressed in the JCIDS process, demonstrated in test & evaluation, and implemented by fielding and sustaining the system. To reach that objective within resource and statutory constraints, trade-offs are continually conducted to balance performance, availability, process efficiency, risks, and cost. This requires the PM to think in both long and short terms.

Short term pressures to achieve system performance and schedule imperatives are very real, and cannot be ignored in a financially and statutorily constrained environment. However, system sustainability and affordability are also important program elements to be considered. Consequently CJCS Instruction 3170.01 established the Sustainment Key Performance Parameter and KSAs to reinforce the total life-cycle approach to program decisions. This is because a system that meets performance requirements but saves acquisition dollars by not expending the resources to make it reliable, maintainable, or supportable is a liability to the user.

Ultimately, over the system life cycle, balancing this composite of long term objectives will provide greater benefit.

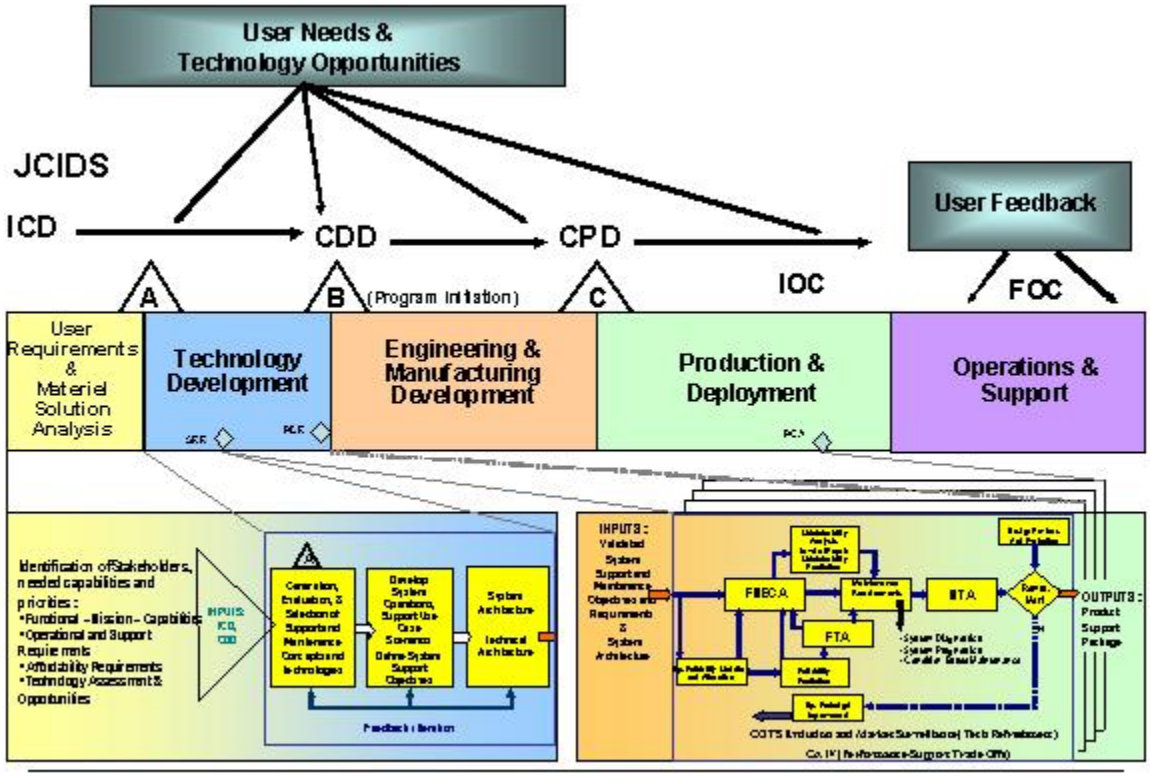


Figure 5.2.F1. Supportability Analysis in Acquisition

Achieving Affordable System Operational Effectiveness. The PM can address the long versus short term issue by designing for the optimal balance between performance (technical and supportability), total ownership costs, schedule, and process efficiency. A development program that targets only some categories of technical performance capability; or fails to optimize system Reliability, Availability, and Maintainability (RAM) technical performance, risks financial burden during operations and support. The PM should therefore design for the optimal balance between technical performance (including RAM), categories of ownership cost, schedule, and process efficiencies. The affordable system operational effectiveness concept is important because it is what the user sees in terms of how well the system is able to perform its missions over a sustained period as well as the ability to surge given the user's operating budget. In this concept the emphasis is not only on the system's ability to execute its mission or its reliability and maintainability, but also on the cost effective responsiveness of the supply chain. The challenge is in how to relate these interrelated elements into an integrated shared vision across the wide range of stakeholders. The major elements impacting a system's ability to perform its mission that should be considered in the design process are depicted in Figure 5.2.F2 and addressed below:

Mission effectiveness is critical because it reflects the Warfighter's ability to accomplish the mission (including the number of systems/sorties required to accomplish the mission) and directly impacts their workload. It reflects the balance achieved between the design and the process efficiencies used to operate and support the system, including the product support package and the supply chain. In addition, each of its elements directly influences the **life-cycle cost / total ownership costs**. The key is to ensure mission effectiveness is defined in terms meaningful to the Warfighter over a meaningful timeframe. (e.g., number of systems required to move X ton miles in a 30 day period, or number of systems required to provide continuous surveillance coverage over 60,000 square mile area for a 6 month period)

The design effectiveness reflects key design features - technical performance and supportability features. These system aspects should be designed-in synergistically and with full knowledge of the expected system missions in the context of the proposed system operational, maintenance, and support concepts. To be effective, technical performance and supportability objectives should be defined in explicit, quantitative, testable terms. This is important to facilitate trade-offs as well as the selection and assessment of the product and process technologies. Each of the major elements controlled by the program manager in the design process is addressed below.

Technical performance is realized through designed-in system functions and their corresponding capabilities. In this context, functions refer to the desired mission abilities the system should be capable of executing in the operational environment. This includes high level functions such as intercept, weapons delivery, electronic jamming, surveillance, etc. down to the lowest subsystem level supporting functions (e.g., process signal). Capabilities refer to the various desired performance attributes and measures, such as maximum speed, range, altitude, accuracy (e.g., "circular error probable") down to the lowest subsystem level (e.g., frequencies). Each of these must be prioritized and traded off to achieve an acceptable balance in the design process.

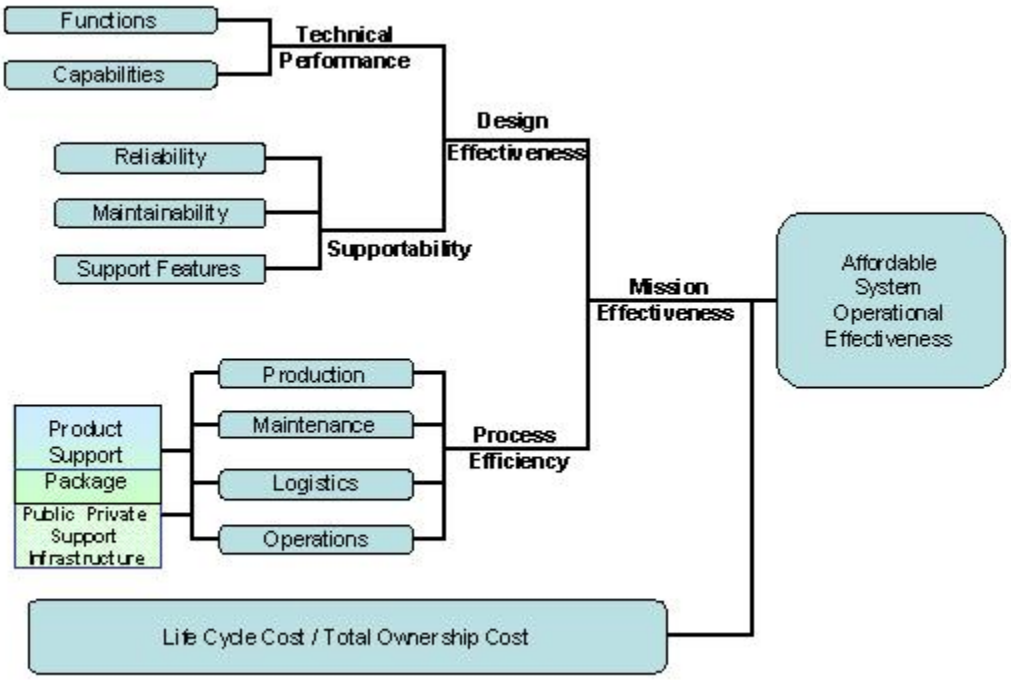


Figure 5.2.F2. Affordable System Operational Effectiveness

In this context, supportability (see sections 5.3 and 4.4.19) includes the following design factors of the system and its product support package:

- **Reliability** is the ability of a system to perform as designed in an operational environment over time without failure.
- **Maintainability** is the ability of a system to be repaired and restored to service when maintenance is conducted by personnel using specified skill levels and prescribed procedures and resources (e.g., personnel, support equipment, technical data). It includes unscheduled, scheduled maintenance as well as corrosion protection/mitigation and calibration tasks.
- **Support features** include operational suitability features cutting across reliability and maintainability and the supply chain to facilitate detection, isolation, and timely repair/replacement of system anomalies. It also includes features for servicing and other activities necessary for operation and support including resources that contribute to the overall support. Traditional factors falling in this category include diagnostics, prognostics (see CBM+ Guidebook), calibration requirements, many HSI issues (e.g. training, safety, HFE, occupational health, etc.), skill levels, documentation, maintenance data collection, compatibility, interoperability, transportability, handling (e.g., lift/hard/tie

down points, etc.), packing requirements, facility requirements, accessibility, and other factors that contribute to an optimum environment for sustaining an operational system.

Supportability features cannot be easily "added-on" after the design is established. Consequently supportability should be accorded a high priority early in the program's planning and integral to the system design and development process. In addition to supportability features, the associated product support package, along with the supply chain, are important because they significantly impact the processes used to sustain the system, allowing it to be ready to perform the required missions. While not specifically identified in figure 5.2.F2, producibility (i.e. the degree to which the design facilitates the timely, affordable, and optimum-quality manufacture, assembly, and delivery) can also impact supportability. This is because easily producible items are normally faster to obtain and have lower total ownership costs.

Process efficiency reflects how well the system can be produced, operated, serviced (including fueling) and maintained. It reflects the degree to which the logistics processes (including the supply chain), infrastructure, and footprint have been balanced to provide an agile, deployable, and operationally effective system. While the program manager does not fully control this aspect, the program directly influences each of the processes via the system design and the fielded product support package. Achieving process efficiency requires early and continuing emphasis on the various logistics support processes along with the design considerations. The continued emphasis is important because processes present opportunities for improving operational effectiveness even after the "design-in" window has passed via lean-six sigma, supply chain optimization and other continuous process improvement (CPI) techniques. Examples of where they can be applied include supply chain management, resource demand forecasting, training, maintenance procedures, calibration procedures, packaging, handling, transportation and warehousing processes.

The relationships illustrated in figure 5.2.F2 are complex and not as clean as shown in the figure. Figure 5.2.F3 is more accurate relative to how the basic system operational effectiveness elements interface. For example, each of the supportability elements influences the process aspects which in turn can impact supportability. (e.g., while reliability drives the maintenance requirements, the implemented maintenance processes and the quality of the spare and repair parts as reflected in the producability features can impact the resultant reliability.) In addition, how the system is operated will influence the reliability and both can be influenced by the logistic processes. Last but not least, each of the design and process aspects drives the life-cycle costs. Achieving the optimal balance across these complex relationships requires proactive, coordinated involvement of organizations and individuals from the requirements, acquisition, logistics, and user communities, along with industry. Consequently, because of the complexity and overlapping interrelationships full stakeholder participation is required in activities related to achieving affordable mission effectiveness. Models that simulate the interactions of the elements, as depicted in Figure 5.2.F3, can be helpful in developing a balanced solution.

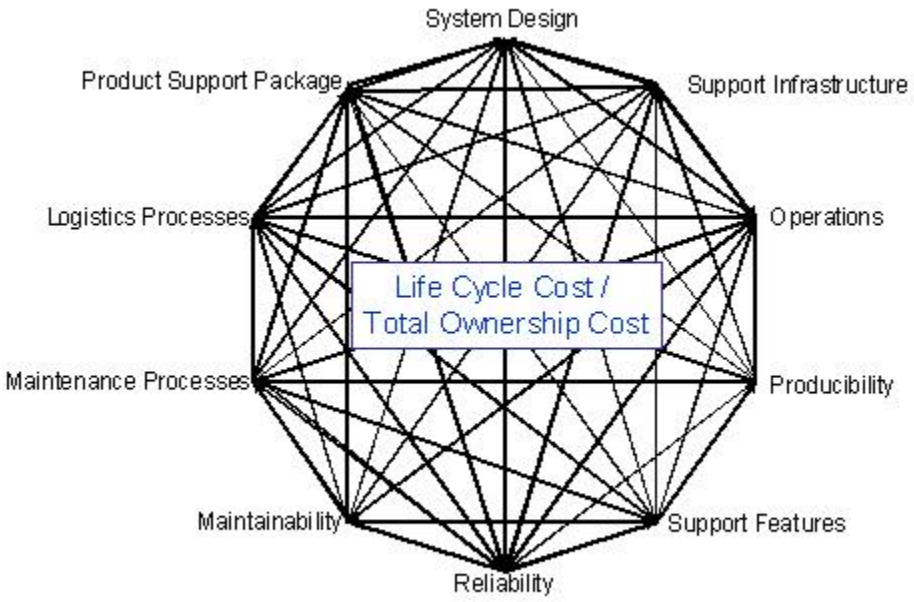


Figure 5.2.F3. Affordable System Operational Effectiveness Interrelationships

Each of the elements reflected in Figure 5.2.F2 contribute to achieving the top level affordable operational effectiveness outcome and have associated metrics which can be measured to assess efficiency and effectiveness. However, they don't mathematically add up as implied in Figure 5.2.F2. This is because, in addition to the complex interrelationships between the elements, the various stakeholders only measure portions of the supply chain and often use different metric definitions. Consequently DoD has adopted 4 key sustainment metrics (including the Sustainment KPP and 2 KSAs) for projecting and monitoring key affordable operational effectiveness performance enablers to:

- Provide a standard set of encompassing measures to continuously estimate and assess affordable operational effectiveness
- Complement the traditional readiness metrics to help overcome the overlapping interrelationships,
- Provide a common communications link across the diverse systems and organizations
- Provide the programs latitude in determining the optimum solution.

Figure 5.2.F4 indicates the minimum set of sustainment metrics the PM should use to facilitate communication across the stakeholders and the elements affecting them. The color code indicates the elements measured by Materiel Availability, Materiel Reliability and Mean Down Time metrics. The metrics are interrelated and along with the CONOPS impact the LCC/total ownership costs.

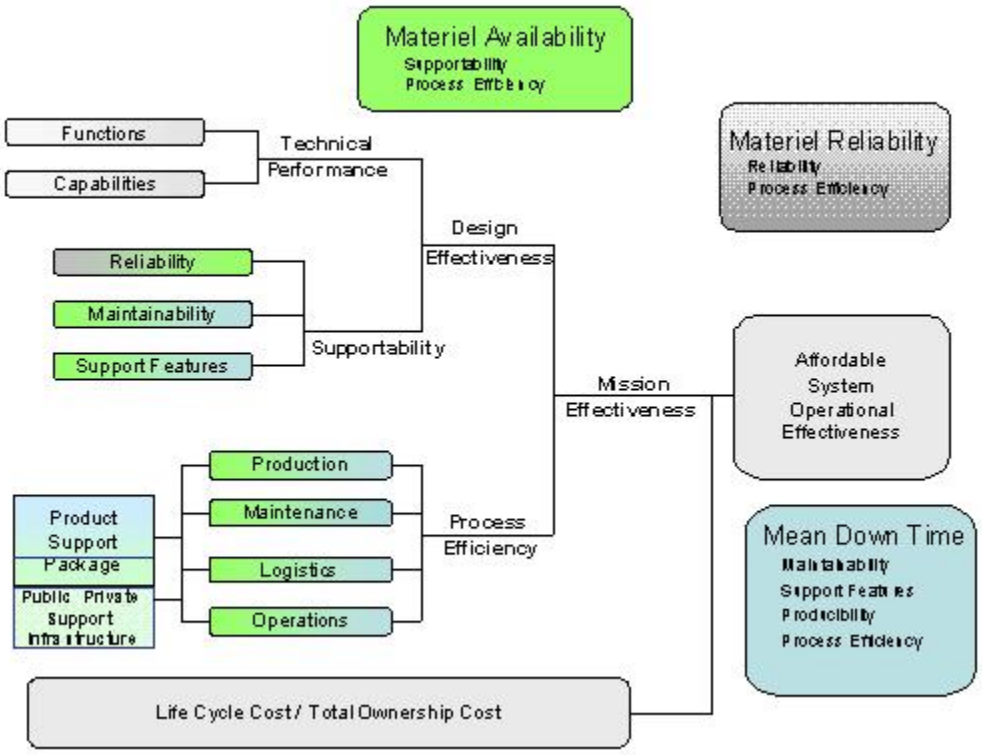


Figure 5.2.F4 Sustainment Metrics & Affordable System Operational Effectiveness

This overarching perspective provides context for the trade space available to a PM and for articulation of the overall objective of maximizing the operational effectiveness. This is critical because trade-offs outside the trade space (i.e., program parameter changes) can require approval of both the Milestone Decision Authority and Validation Authority since validated KPP threshold values cannot be reduced without Validation Authority approval. Consequently, it is critical the design trade space established by the values selected for the sustainment metrics be established early and be acceptable to the user and acquirer communities. As a result, the user and sponsor should be involved with the determination of the design trade space. Finally, to help ensure the metrics goals are met, the program should establish supporting metrics for key drivers (e.g., logistics footprint, manning levels, ambiguity rates for diagnostics) uniquely tailored for the system and the projected operating environment as the design requirements are allocated.

5.2.1. Supportability Analysis

5.2.1.1. Supportability Analysis Phases

5.2.1.2. Supportability Analysis Steps

5.2.1.3. Key Depot Maintenance Analysis Elements

5.2.1. Supportability Analysis

Sustainment requirements should be an integral part of the systems engineering design process. (A detailed discussion of the systems engineering process can be found in section 4.2.) Regardless of the life-cycle phase, effective supportability begins with the development of sustainment requirements to drive the design and development of reliable, maintainable and affordable systems through the continuous application of the systems engineering methodology focusing on affordable system operational effectiveness. The key is to smoothly integrate the systems engineering processes and design maturation processes together with the Defense Life-Cycle Management System and its milestones. A key product of the supportability analysis is the maintenance plan which evolves and drives all sustainment resource requirements throughout the life cycle.

5.2.1.1. Supportability Analysis Phases

Section 5.4 provides areas of focus for each acquisition phase. In general, however, life-cycle management can be thought of in terms of three broad periods.

- **Pre-Systems Acquisition:** Determining the capabilities and major constraints (cost, schedule, available technology) that frame the acquisition strategy and program structure for both the system and its support concept
- **Acquisition:** Designing, producing and deploying the equipment and its support system
- **Operations:** Adjusting to the operational environment by assessing readiness trends/issues, cost trends, evolving materiel conditions, and taking timely corrective actions to support the users

Pre-Systems Acquisition: Here, supportability analysis should be used to evaluate the suitability of material alternatives, shape life-cycle sustainment concepts and determine the product support capability requirements. Each alternative should be assessed to determine the likely materiel availability and its life-cycle affordability. Generally the analysis starts at the system level but can selectively go to lower levels of indenture if key enabling technologies are required to meet the CONOPS (for both the system and the product support system). This includes using supportability analysis to:

- Evaluate alternatives until an optimum balance is achieved between mission effectiveness and the KPPs (including the Sustainment KSAs). Specifically it should be used to ensure the preferred System Concept & Support CONOPS, are consistent with the projected Operational CONOPS taking into account "real world" constraints including "core", statutory requirements, existing supply chain, etc. Generally this is done by considering the sustainment effectiveness and O&S affordability of systems currently performing the same or similar capabilities. These are analyzed and serve as benchmarks to assess alternatives; with the intent of incremental improvement over current (legacy) system capability readiness and cost.

- Evaluate product support capability requirements using a notional Support CONOPS for trades and LCC estimates in evaluating the alternatives.
- Identify enabling sustainment technology needed to meet life-cycle sustainment goals especially when the risk of achieving the incremental improvements is high (e.g., a robust software architecture, health management, diagnostics, prognostics. etc.).
- Assess the operational and life-cycle risks associated with sustainment technologies, especially those requiring development.
- Integrate supportability performance into systems engineering, initial acquisition strategic planning, and as benchmark criteria for test and evaluation.
- Refine associated performance requirements based on technology development results (positive and negative) to achieve the preferred system concept & Support CONOPS.
- Refine supportability performance requirements and life-cycle sustainment concepts, based on evolving technology and changes in the CONOPS.

Acquisition: Here, supportability analysis helps reduce risks and create/field the system and its supply chain with provided feedback into the design process. This is accomplished by assessing the affect of system plans, development, and production on sustainment effectiveness, readiness, and O&S affordability. The intent is to act early to mitigate evolving circumstances that may adversely impact deployed readiness. This includes using systems engineering in designing the system and its supply chain; producing both concurrently; and testing to verify the total system requirements have been achieved. Specifically systems engineering is used in designing for support and:

- Taking Warfighter requirements (Including the Operational CONOPS) and developing the sustainment objectives, Support and Maintenance CONOPS and determining their detailed "design-to" and "build to" requirements. (It also includes identifying the performance requirements for the supporting supply chain segments to support the Operational CONOPS.) In accomplishing this, the trades/analyses are used to identify:
    - The key metric values (e.g., the drivers) required to meet the operational/campaign model assumptions/requirements as well as the impact on Warfighter mission capability (e.g., ability to generate a mission (operational readiness) and perform during a mission) of the various trades.
    - LCC drivers for the system, its support concept and maintenance concept/plan.
    - The optimum mix of driver values to meet KPPs and their corresponding confidence levels.
    - Effectiveness (KPP/KSA Outcomes) if the supply chain performs at today's levels (as well as if current trends continue or with anticipated trends).
- Taking the test/initial operations results and predicting likely mature values for each of the KSA and enabler drivers.
- Providing integrated Sustainment KPP/KSA estimates into the Defense Acquisition Management Information Retrieval (DAMIR) system.

During this period more realistic and detailed data is used in the models/simulations to reduce risk and define achievable performance & sustainment requirements. Consequently, a mix of

design estimates/contract requirements, sustainment, and Maintenance Plan metrics are used when conducting sustainment trades/analysis depending on the period and objective. In addition, expected trends for system, enabler & supply chain metrics and their confidence levels are also needed requiring the use of data models. This requires that:

- Data realism is based on systems engineering/technology assessments.
- Metric values can be evaluated and re-adjusted as necessary.
- The required data elements performance requirements can be defined in contract terms.
- There is a means to verify the maturity growth over time.

Operations: Here, supportability analysis is used to help in adjusting the program based on the sustainment program's achieved effectiveness as well as on changing hardware and operational conditions. This includes using supportability analysis to:

- Analyze the impact of proposed re-design alternatives on the sustainment metrics and mission effectiveness.
- Analyze the impact of proposed process changes on the sustainment metrics.
- Take use data and user feedback including Failure & Discrepancy Reports to:
    - Project trends (with confidence levels) so proactive actions are taken as conditions warrant to minimize adverse impacts on the users.
    - Identify areas in the supply chain where performance is adversely affecting materiel availability, increasing ownership costs or missing areas of potential savings/improvements. (Note, that care is needed, since, in some cases, an increase within a specific system may be significantly offset by a major saving elsewhere within the DoD Component or DoD. Consequently, higher level organizations may have to be engaged in the final decision.)
    - Identify and analyze readiness risk areas and develop corrective action alternatives.
- Relate/quantify various business process outcomes with resources.

During this period, the system program measures and tracks the supply chain and its effectiveness and use models that include the driver metrics to determine root causes of problems or anticipate future problems.

5.2.1.2. Supportability Analysis Steps

As discussed in section 4.4, designing for optimal system affordability and operational effectiveness requires balance between mission effectiveness and life-cycle cost. The emphasis is not only on the reliability and maintainability of the system to achieve mission capability, but also on human systems integration and optimization of all human interfaces across the HSI domains to ensure the cost-effective responsiveness and relevance of the support systems and supply chain. This is critical since a majority of ownership costs are human related and are locked in early in the acquisition life cycle. Consequently it is important that a comprehensive HSI program be initiated early in the life cycle to address the major ownership cost drivers.

These objectives can best be achieved through integration with the system design and CONOPS (both operational and sustainment) and by focusing on the sustainment requirements. As depicted in Figure 5.2.1.2.F1, the supportability analysis process is most effectively carried out through inclusion from the very beginning of a program - starting with the definition of required capabilities.

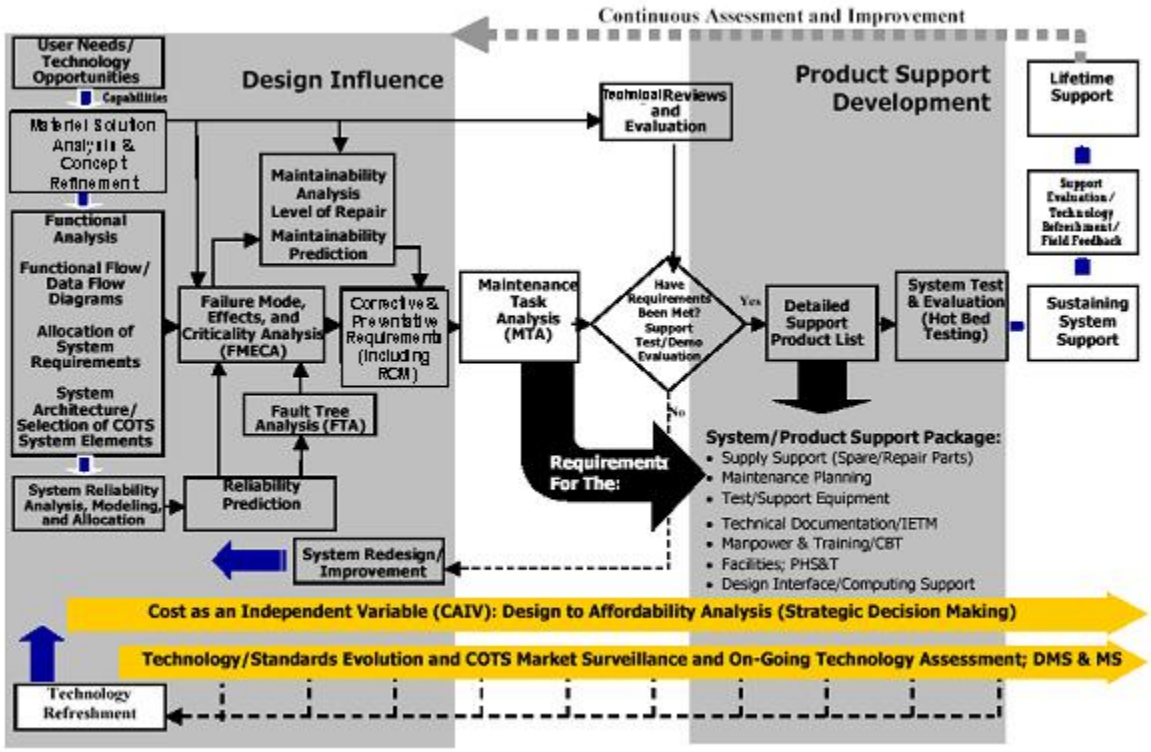


Figure 5.2.1.2.F1. Supportability Relationships

Implementation of a disciplined supportability analysis approach, including systems engineering activities such as CBM+, Failure Mode Effects and Criticality Analysis (FMECA), Fault Tree Analysis (FTA), Reliability Centered Maintenance (RCM) (see Enclosure 3, DoDI 4151.22 RCM Process), and level of repair analysis (considering cost and availability implication of the maintenance level and locations) will produce a Maintenance Task Analysis (MTA) directly linked to the system's reliability and maintainability characteristics. The Maintenance Task Analysis is the opportunity to determine whether the design has met the supportability requirements defined in the system specification, and provides a feedback loop to the Systems Engineer that is either positive (design has met requirements) or that there is a need for re-evaluation of either the requirement or the design itself. The results of the re-evaluations permits the trade space required for the PM to make a justifiable decision. The RCM analytical process which determines the preventive maintenance tasks is critical in providing recommendations for actions necessary to maintain a required level of safety, maximize materiel availability, and minimize operating cost. In addition to DoD Component guides and handbooks (e.g. MIL-P-

24534A), SAE JA1011 (Evaluation Criteria for RCM Programs) and SAE JA1012 (A Guide to the RCM Standard) are illustrative commercial standards for this method.

The technical input and maintenance task analysis provide a detailed understanding of the necessary logistics support element requirements to sustain required materiel availability. The MTA process identifies support tasks and the physical location where they will be accomplished considers the costs, availability implications, and statutory requirements. (The Depot Source of Repair (DSOR) process is key in determining location.) This in turn produces a product support package that identifies support element requirements and associated product data based on the system reliability and maintainability. The product support package provides descriptions of the following topics:

- Supply Support (Spare/Repair Parts)
- Maintenance Plan and Requirements
- Support, Test & Calibration Equipment
- Technical Data (Paper Based and/or Electronic Interactive)
- Manpower & Training including Computer Based Training
- Facility Requirements
- Packaging, Handling, Storage, & Transportation
- Computer Resource Support

The steps shown in figure 5.2.1.2.F1 are not necessarily carried out in a linear progression. Design increments and the continuous assessment of test results and in-service system performance will identify needs for system improvements to enhance reliability, and maintainability and to overcome obsolescence, corrosion, or other sustainment problems. Additional information including a detailed process description, considerations in implementing the process and data element definitions, can be found in MIL-HDBK-502.

5.2.1.3. Key Depot Maintenance Analysis Elements

Program managers should analytically determine the most effective levels of maintenance and sources based on materiel availability and cost factors. 10 U.S.C. 2464 and DoD policy require organic core maintenance capabilities be in place to provide effective and timely response to surge demands and to ensure cost efficiency and technical competence. In addition per 10 USC 2464, core sustaining workload must be accomplished in Government owned facilities with Government owned equipment and personnel. The PM should perform an analysis to determine the maintenance source that complies with statutory requirements, operational readiness and best value for non core workloads. (Initial organic depot maintenance source of repair assignments must employ merit-based selection procedures to select among alternative sources. Depot maintenance workloads previously accomplished at organic facilities, with a value of at least three million dollars, must also be subjected to merit-based selection procedures when deciding between alternative organic sources of repair. Additional information including exceptions to the requirement can be found in DoDD 4151.18 and DoD Instruction 4151.20.)

Core Logistics Capability. Title 10 U.S.C. 2464 and DoDI 4151.20 require core logistics capability that is government-owned and government-operated (including government personnel and government owned and operated equipment and facilities) to ensure a ready and controlled source of technical competence with the resources necessary to ensure effective and timely response to mobilization, national defense contingency situations, or other emergency requirements. These capabilities must be established no later than 4 years after achieving IOC. These capabilities should include those necessary to maintain and repair systems and other military equipment that are identified as necessary to fulfill the strategic and contingency plans prepared by the Chairman of the Joint Chiefs of Staff. (Excluded are special access programs, nuclear aircraft carriers, and commercial items, as defined by (Title 10 U.S.C. 2464).) Core logistics capabilities should be performed at government owned-government operated (GO-GO) facilities of a military department. Such facilities should be assigned sufficient workload to maintain these core capabilities and ensure cost efficiency and technical competence in peacetime while preserving the surge capacity and reconstitution capabilities necessary to fully support strategic and contingency plans.

Depot Source of Repair (DSOR) Analysis. The process to help the PM select the best value in depot maintenance support is implemented through the Depot Source of Repair (DSOR) analysis. The Depot Source of Repair Guide provides additional information for accomplishing the required Core Logistics Analysis/Source of Repair Analysis in determining the source of repair for depot level workload. The DSOR decision process is an integral part of sustainment planning and mandatory for systems/equipment requiring depot maintenance. DoD Directive 4151.18, Maintenance of Military Materiel, requires DSOR assignments be made by the PM using the DSOR assignment decision logic. The process should be completed before entering into firm commitments or obligating funds for other than interim depot support. The DSOR decision is typically made during the Engineering & Manufacturing Development and the Production and Deployment phases.

The DSOR decision process consists of two major elements, normally performed sequentially: The first is the organic versus contract source of repair determination. This determination is made by the PM using a DoD Component approved analysis process that gives consideration to core requirements. Title 10 USC 2464, Core Logistics Capabilities; Title 10, USC 2466, Limitations on the Performance of Depot Level Maintenance of Materiel, and DoD Directive 4151.18 provide further guidance for this process.

The second element in the DSOR decision process is consideration of interservice depot maintenance support. This element, known as the Depot Maintenance Interservice (DMI) review, is required regardless of the outcome of the contract versus organic selection. The DMI review is prescribed in the Joint Depot Maintenance Program regulation Logistics, Joint Depot Maintenance Program with individual DoD Component details spelled out in OPNAVINST 4790.14A, AMC-R 750-10, AFI 21-133(I), MCO P4790.10B, and DLAD 4151.16. All new acquisitions, equipment modifications, and items moving to or from contract depot maintenance support are to be reviewed for interservice potential in accordance with this regulation.

The DSOR decision process has the potential to reduce program costs by effectively using commercial and organic depot maintenance resources. The process helps ensure the DoD Components maintain the core depot maintenance capability, as required by statute that meets military contingency requirements and considers interservice depot maintenance support and joint contracting. In performing this analysis, the PM should ensure that maintenance source of support decisions comply with the following statutory requirements:

Depot Maintenance 50 Percent Limitation Requirement. Title 10 U.S.C. 2466 requires not more than 50 percent of the funds made available in a fiscal year to a military department or defense agency for depot level maintenance and repair workload as defined by Title 10 U.S.C. 2460 be used to contract for performance by non-federal government personnel. As this is a military department and agency level requirement and not a system specific requirement, the PM should not undertake depot maintenance source of support decisions without consultation with accountable military department logistics officials to get the DoD Component position on this statutory requirement.

5.2.2. Life-Cycle Costs (LCC) and Total Ownership Costs (TOC)

LCC is the cost to the government to acquire and own a system over its useful life. It includes all life-cycle management costs (e.g. development, acquisition, operations, support, and disposal). Total ownership cost consists of the elements of a program's life-cycle cost, as well as other supply chain or business processes costs that logically can be attributed to the operation of a system. Section 3.1.5 provides additional information but generally TOC can be thought of as expansion of the "indirect cost" elements. For example, it could include such costs as delivering fuel/batteries, recruiting/ accession training of new personnel, individual training, environmental and safety compliance, management headquarters functions, etc.

Early program decisions ultimately determine the LCC and drive the total ownership costs, the majority of which is incurred after a system is deployed,. Consequently beginning with the requirements determination and during each life-cycle phase, LCC estimates should play a major role in the program decision process for evaluating affordable alternatives during the design and trade-off processes. (See DoD Directive 5000.01, E1.1.4, E1.1.17, and E1.1.29.) As a result, ownership cost is now treated as a military requirement via the JCIDS's Ownership Cost KSA. For this reason, LCC should be treated as an independent variable (see section 3.2.4) and analysis should be performed to the level appropriate for the decision and alternatives considered. However, since projections are based on assumptions, cost estimates shall include an assessment of confidence levels and should also include the associated cost drivers.

In general, traditional life-cycle cost estimates are adequate in scope to support decisions involving system design characteristics, with indirect cost elements being handled via standard cost factors/surcharges/burdened rates. However, in special cases depending on the issue, the broader perspective of total ownership cost may be more appropriate than just the traditional life-cycle cost elements a program can directly influence. For example, when determining the materiel solution to meet requirements (e.g., manned vs. unmanned, or space based vs. ship

based, etc) TOC elements dealing with the supply chain will need to be considered since each materiel solution has a significantly different cost impact to the tax payer. During the design and sustainment phases, indirect TOC elements may also be broken out rather than using cost factors when considering decisions directly impacting the wholesale logistics infrastructure processes. Examples of these types include decisions dealing with required skill levels to maintain the system, alternative system support concepts and strategies, reengineering of business practices or operations, and competitive sourcing of major supply chain activities.

Life-cycle cost analysis can be very effective in reducing the total ownership cost of the system and its support strategy. (Within DoD, reduction and control of LCC is also done through a variety of initiatives including Value Engineering (see section 4.5.5), Reduction of Total Ownership Costs (RTOC), etc.) However, one cost model is not sufficient to address all of the alternatives a PM must consider. The level of detail, analysis process used, and LCC elements considered should be tailored to the decision being made, focusing on cost drivers and costs that will be incurred by the government and not just on direct program office costs.

For most decisions, the sunk costs, costs that will not be impacted by the alternatives and absolute value of the alternatives can be ignored. The analysis should be focused instead on the relative cost element differences between the alternatives considered and the cost drivers for each. Consequently, in many cases other key sustainment related cost performance criteria, such as O&S cost-per-operating-hour, can be considered in implementing cost as an independent variable (CAIV) principles. The Cost Analysis Requirements Description (see section 3.4.4.1) reflects the life-cycle sustainment requirements for preparing the LCC estimate and the Cost Analysis Improvement Group Operating and Support Cost Estimating Guide also provides useful information relative to the cost estimating process, approach, and other considerations.

5.2.3. Sustainment Modeling and Simulation (M&S)

M&S can be an effective tool in the supportability analysis and evaluation process in implementing life-cycle management principles because all the sustainment/materiel readiness driver metrics can be considered in parallel (also see section 4.5.8). Consequently, the sustainment M&S objective should be to use validated models to consider materiel availability/readiness implications when assessing the merits of alternatives throughout the life cycle. M&S should be used in assessing the alternatives for major decisions affecting the design and deployment of both the end item and its support system. Properly applied M&S encourages collaboration and integration among the varied stakeholders (including the test and transportation communities) facilitating materiel availability and system effectiveness.

The models should be used throughout the life cycle and should include the multiple materiel availability stakeholder contribution and funding streams for the supply chain components. (The level of detail used varies based on several factors including, but not limited to, the system's complexity, criticality to the user, program phase, and risk.) In all cases, M&S efforts should consistently and credibly look at/trade off life-cycle alternatives in a repeatable fashion. In addition, the underlying assumptions and drivers for the values of each of the sustainment

metrics should be documented as thresholds, objectives, and estimates evolve through the life cycle. (See the RAM-C Guide for additional information.)

5.2.4. Process Models

M&S and continuous process improvement initiatives are dependent on defined processes. The government and industry have undertaken a series of initiatives to define generic multi level processes with associated metrics that might prove useful when developing new analysis models. The following general models have been developed.

The Supply Chain Operations Reference (SCOR) model, figure 5.2.4.F1, captures a consensus view of the supply chain plan, source, maintain/make, deliver, and return, processes in a framework linking business process, metrics, best practices, and technology features into a unified structure for effective supply chain management and for improving related supply chain activities. In this context, the supply chain includes the transportation and maintenance chains as well as the spare/repair parts chain required to provide the user flexible and timely materiel support during peacetime, crises, and joint operations. Most of these supply chain activities are governed by DoD regulation 4140.1-R, Supply Chain Materiel Management Regulation which provides further DoD guidance and information. Maintenance requirements within the supply chain are governed by DoD Directive 4151.18, Maintenance of Military Materiel.

Building off the SCOR efforts, the **Design Chain Operations Reference (DCOR)** model links business process, metrics, best practices and technology features into a unified structure to support communication among design chain partners and to improve the effectiveness of the extended supply chain. The model is organized around five primary management processes which focus on product development and research & development. As is in the case of SCOR, this consensus model can be used to describe design chains can be simple or complex using a common set of definitions.

The **Customer Chain Operations Reference (CCOR)** model captures a consensus view of the feedback processes including the health and welfare of the customer supplier relationship. This model is the least mature and also undergoing refinement by practitioners. However, combined and tailored, the 3 models can provide an end to end view of the entire enterprise wide process covering processes, activities and metrics.

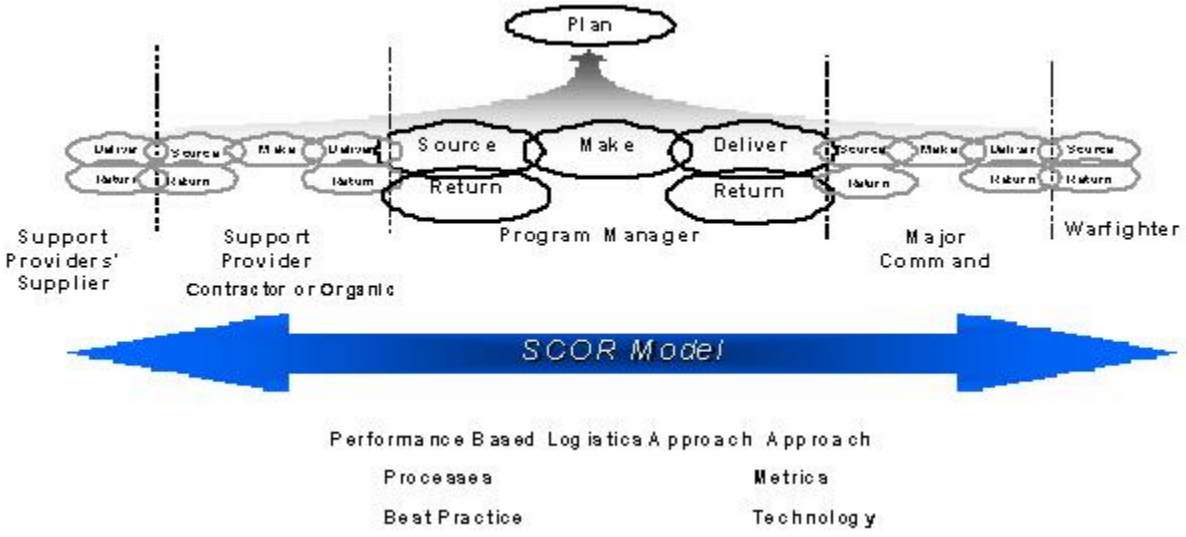


Figure 5.2.4.F1. The Supply Chain Operations Reference (SCOR) Model

5.3. Supportability Design Considerations

Logistics Infrastructure and Footprint Reduction. Programs can best support evolving military strategy by providing forces with the best possible system capabilities while minimizing the logistics footprint. Consequently, programs are responsible for achieving program objectives throughout the life cycle while minimizing cost and logistics footprint (see DoD Directive 5000.01, E1.17 and E1.29). To achieve these goals, the support posture of a system needs to be designed-in up front (i.e., logistics and availability degraders are designed out) since the opportunities for decreasing the logistics footprint decline significantly as the system evolves from design to production to deployment. Minimizing the logistics footprint through deliberate and integrated logistics/engineering design efforts means that a deployed system will require fewer quantities of support resources especially:

- Spares and the supply chain
- Test, support and calibration equipment
- Manpower and personnel requirements (including highly specialized or unique skill/ training requirements)
- System documentation/technical data

Sustainment analyses should include a basic understanding of the concept of operations, system missions, mission profiles, and system capabilities to understand the rationale behind functional and performance priorities. Understanding the rationale paves the way for decisions about necessary trade offs between system performance, availability, and LCC, with impact on the cost effectiveness of system operation, maintenance, and logistics support. There is no single list of sustainment considerations or specific way of grouping them as they are highly inter-related.

They range from: compatibility, interoperability; transportability; reliability; maintainability; manpower; human factors; safety; natural environment effects (including occupational health; habitability); diagnostics & prognostics (including real-time maintenance data collection); and corrosion protection & mitigation. The following are key considerations that should be considered for the System Specification.

5.3.1. Architecture Considerations

Figure 5.3.1.F1 lists key system architecture attributes which can provide a solid sustainment foundation. The focus on openness, modularity, scalability, and upgradeability is critical to implementing an incremental acquisition strategy. In addition, the architecture attributes that expand system flexibility and affordability can pay dividends later when obsolescence and end-of-life issues are resolved through a concerted technology refreshment strategy. However trade-offs are required relative to the extent each attribute is used as illustrated in the Commercial Off-the-Shelf (COTS) case.

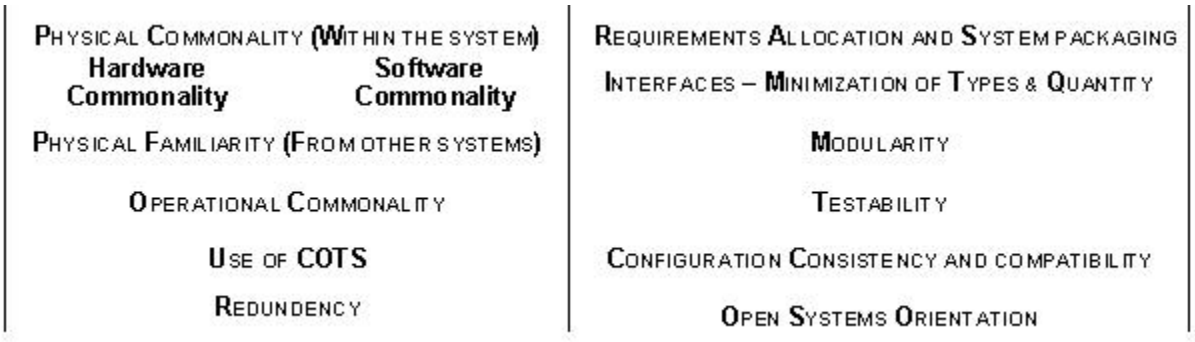


Figure 5.3.1.F1. Illustrative attributes for System Architecture Supportability Assessments

Maturity and use of Commercial Off-the-Shelf (COTS) Items. Technology risk should receive consideration as the system is developed. Maximum use of mature technology (including non-developmental and/or standards based COTS software or computer hardware) provides the greatest opportunity to adhere to program cost, schedule, and performance requirements by leveraging industry's research & development and is consistent with an incremental acquisition approach. However, this is not a one time activity. Unanticipated changes and the natural evolution of commercial items may drive reconsideration of engineering decisions throughout the life cycle. In addition, the program must consider the logistics implications of supporting commercial items in a military environment. Finally, because COTS items have a relatively short manufacturing life, a proactive diminishing manufacturing sources and material shortages / obsolescence approach should also be considered. Consequently, care must be taken to assess the long term sustainability of COTS options and to avoid or minimize single source options.

Modular Open Systems Approach (MOSA). Open system architectures help mitigate the risks associated with technology obsolescence and promote subsequent technology infusion. MOSA

can also help to provide interoperability, maintainability, and compatibility when developing the support strategy and follow-on logistics planning for sustainment. It can also enable continued access to cutting edge technologies and products and prevent being locked into proprietary technology. Applying MOSA should be considered as an integrated business and technical strategy when examining alternatives to meet user needs. PMs should assess the feasibility of using widely supported commercial interface standards in developing systems. MOSA should be an integral part of the overall acquisition strategy to enable rapid acquisition with demonstrated technology, incremental and conventional development, interoperability, life-cycle sustainment, and incremental system upgradeability without major redesign during initial procurement and re-procurement.

Parts Management. Parts management is a design strategy that seeks to reduce the number of unique, specialized, and defined problem parts used in a system (or across systems) to enhance standardization, commonality, reliability, maintainability, and supportability. In addition to reducing the need and development of new logistics requirement (e.g. documentation) it reduces the logistics footprint and also mitigates parts obsolescence occurrences due to diminishing manufacturing sources and material shortages.

Materiel and Interoperability/Joint Architecture. The Materiel and Interoperability/Joint Architecture concept can be used to help reduce the logistics footprint. (For further discussion on this topic see Chapter 7.)

5.3.2. Reliability

Reliability is critical because it contributes to a system's war fighting effectiveness as well as its suitability in terms of logistics burden and the cost to fix failures. For each system, there is a level of basic reliability that must be achieved for the system to be militarily useful, given the intended CONOPS. Reliability is also one of the most critical elements in determining the logistics infrastructure and footprint. Consequently, system reliability should be a primary focus during design (along with system technical performance, functions, and capabilities). The primary objective is to achieve the necessary probability of mission success and minimize the risk of failure within defined availability, cost, schedule, weight, power, and volume constraints. While performing such analyses, trade-offs should be conducted and dependencies should be explored with system maintainability and integrated with the supportability analysis that addresses support event frequency (i.e. Reliability), event duration and event cost. Such a focus will play a significant role in minimizing the necessary logistics footprint, while maximizing system survivability and availability.

The requirements determination process offers the first opportunity to positively influence a system from a reliability perspective. Trade-offs among "time to failure," system performance, and system life-cycle cost are necessary to ensure the correct balance and to maximize materiel availability. Options that should be considered and implemented to enhance system reliability and achieve the Materiel Reliability KSA include:

- Over-designing to allow a safety margin;
- Redundancy and/or automatic reconfiguration upon failure allowing graceful degradation;
- Fail safe features (e.g., in the event of a failure, systems revert to a safe mode or state to avoid additional damage and secondary failures). Features include real time reprogrammable software, or rerouting of mission critical functions during a mission;
- Calibration requirements; and
- Reliability Growth Program.

Reliability estimates evolve over time. Generally, the initial estimates are based on parametric analyses and analogies with like or similar systems operating in the same environment and adjusted via engineering analysis. As the design evolves and as hardware is prototyped and developed, the engineering analysis becomes more detailed. In addition to estimates and modeling, testing at the component, subsystem, or system level may be necessary to assess or improve reliability. Approaches such as accelerated life testing, environmental stress screening, and formal reliability development/growth testing, should be considered and incorporated into program planning as necessary. To assure the delivery of a system that will achieve the level of reliability demanded in field use, a methodical approach to reliability assessment and improvement should be a part of every well-engineered system development effort. The Reliability Availability and Maintainability (RAM) Guide provides a structure, references, and resources to aide in implementing a sound strategy. It is crucial the reliability approach be planned to produce high confidence the system has been developed with some margin beyond the minimum (threshold) reliability. This will allow for the inevitable unknowns that result in a decrease between the reliability observed during development and that observed during operational testing and in-service. In addition to reliability, the Reliability, Availability, Maintainability & Cost (RAM-C) Rationale Report Manual provides guidance in how to develop and document realistic sustainment Key Performance Parameter (KPP)/Key System Attribute (KSA) requirements with their related supporting rationale; measure and test the requirements; and manage the processes to ensure key stakeholders are involved when developing the sustainment requirements.

5.3.3. Maintainability

The design emphasis on maintainability is to reduce the maintenance burden and supply chain by reducing the time, personnel, tools, test equipment, training, facilities and cost to maintain the system. Maintainability engineering includes the activities, methods, and practices used to design minimal system maintenance requirements (designing out unnecessary and inefficient processes) and associated costs for preventive and corrective maintenance as well as servicing or calibration activities. Maintainability should be a designed-in capability and not an add on option because good maintenance procedures cannot overcome poor system and equipment maintainability design. The primary objective is to reduce the time it takes for a properly trained maintainer to detect and isolate the failure (coverage and efficiency) and affect repair. Intrinsic factors contributing to maintainability are:

- **Modularity:** Packaging of components such that they can be repaired via remove and replace action vs. on-board repair. Care should be taken not to "over modularize" and trade-offs to evaluate replacement, transportation, and repair costs should be accomplished to determine the most cost effective approach.
- **Interoperability:** The compatibility of components with standard interface protocols to facilitate rapid repair and enhancement/upgrade through black box technology using common interfaces. Physical interfaces should be designed so that mating between components can only happen correctly.
- **Physical accessibility:** The designed-in structural assurance that components requiring more frequent monitoring, checkout, and maintenance can be easily accessed. This is especially important in Low Observable platforms. Maintenance points should be directly visible and accessible to maintainers, including access for corrosion inspection and mitigation.
- Designs that require **minimum preventative maintenance** including corrosion prevention and mitigation. Emphasis should be on balancing the maintenance requirement over the life cycle with minimal user workload.
- **Embedded training and testing**, with a preference for approved DoD Automatic Test Systems (ATS) Families when it is determined to be the optimal solution from a TOC and Materiel Availability perspective.
- **Human Systems Integration (HSI)** to optimize total system performance and minimize life-cycle costs. (For further discussion, see Chapter 6 and section 4.4.8.) This includes all HSI domains (Manpower, Personnel, Training, Human Factors Engineering, Environment, Safety, Occupational Health, Survivability, and Habitability) to design systems and incorporate technologies that require minimal manpower, provide effective training, can be operated and maintained by users, are suitable (habitable and safe with minimal environmental and occupational health hazards), and survivable (for both the crew and the equipment).

Condition Based Maintenance Plus. When it can support the materiel availability, prognostics & diagnostics capabilities/technologies should be embedded within the system when feasible (or off equipment if more cost-effective) to support condition based maintenance and reduce scheduled and unscheduled maintenance. Health management techniques can be very effective in providing maintainers with knowledge, skill sets, and tools for timely maintenance and help reduce the logistics footprint. Condition based maintenance plus (CBM+) (the application of technologies, processes, and procedures to determine maintenance requirements based, in large part, on real time assessment of system condition obtained from embedded sensors), coupled with reliability centered maintenance can reduce maintenance requirements and reduce the system down time. (CBM+ references include the DoDI 4151.22, the CBM+ Guidebook, and the CBM+ DAU Continuous Learning Module (CLL029).) The goal is to perform as much maintenance as possible based on tests and measurements or at pre-determined trigger events. A trigger event can be physical evidence of an impending failure provided by diagnostic or prognostics technology or inspection. An event can also be operating hours completed, elapsed calendar days, or other periodically occurring situation (i.e., classical scheduled maintenance). Key considerations in implementing this concept include:

- Use of **diagnostics** monitoring/recording devices and software (e.g., built-in test (BIT) and built-in-self-test (BIST) mechanisms) providing the capability for fault detection and isolation, (including false alarm mitigation) to signal the need for maintenance. It should include user friendly features to convey system status and the effect on mission capabilities to the operator and maintainer.
- Use of **prognostics** monitoring/recording devices and software monitoring various components and indicate out of range conditions, imminent failure probability, and similar proactive maintenance optimization actions to increase the probability of mission success and anticipate the need for maintenance. (As in the case for diagnostics prognostics includes BIT and BIST mechanisms with user friendly features and false alarm mitigation.)
- Maintenance strategies that balance scheduled (preventive) maintenance and minimize unscheduled corrective maintenance with risks.

Key characteristics in implementing the CBM+ concept include:

- Hardware—system health monitoring and management using embedded sensors; integrated data
- Software—decision support and analysis capabilities both on and off equipment; appropriate use of diagnostics and prognostics; automated maintenance information generation and retrieval
- Design—open system architecture; integration of maintenance and logistics information systems; interface with operational systems; designing systems that require minimum maintenance; enabling maintenance decisions based on equipment condition
- Processes—RCM analysis; a balance of corrective, preventive, and predictive maintenance processes; trend-based reliability and process improvements; integrated information systems providing logistics system response; CPI; Serialized Item Management (SIM)
- Communications—databases; off-board interactive communication links
- Tools—integrated electronic technical manuals (i.e., digitized data) (IETMs); automatic identification technology (AIT); item-unique identification (IUID); portable maintenance aids (PMAs); embedded, data-based, interactive training
- Functionality—low ambiguity fault detection, isolation, and prediction; optimized maintenance requirements and reduced logistics support footprints; configuration management and asset visibility.

In accordance with DoDI 4151.22, it is envisioned that elements of CBM+ should be revisited as the life cycle progresses, conditions change, and technologies advance. Consequently CBM+ should be considered and revisited in each life-cycle phase. See CBM+ Guidebook, Section 4 which provides basic steps for planning and implementing CBM+ throughout the life cycle.

5.3.4. Other Logistics Technologies

Program managers can minimize life-cycle cost while achieving readiness and sustainability objectives through a variety of methods in the design of the system and its maintenance / sustainment program. Below are technologies that should be considered to improve maintenance agility and responsiveness, increase materiel availability, and reduce the logistics footprint:

- **Serialized Item Management (SIM).** SIM (DoDI 4151.19) can be used to aid asset visibility and the collection and analysis of failure and maintenance data. (Also see section 4.4.21) The SIM program should be structured to provide accurate and timely item related data that is easy to create and use. While SIM is a DoD wide initiative, the primary function for the program is in ensuring the marking of the population of select items (parts, components, and end items) with a universal item unique identifier (IUID) (DoDI 8320.04). IUID should be used on tangible property, including new equipment, major modifications, and re-procurement of equipment and spares. As a minimum populations from the following categories should be considered for marking:
    - Repairable items down to and including sub-component repairable unit level;
    - Life limited, time controlled, or items with records (e.g., logbooks, equipment service records, Safety Critical Items); and
    - Items that require technical directive tracking at the part number level.

Serialized item management techniques including the use of automatic identification technologies (AIT) such as item unique identification (IUID) technology, and radio frequency identification (RFID) using data syntax and semantics should conform to International Organization for Standardization (ISO) 15418 and ISO 15434.

- **Automatic Identification Technology.** AIT is an integral element of serialized item management programs. IUID markings and accompanying AIT capabilities facilitate paperless identification, automatic data entry, and digital retrieval of supply and maintenance related information. The program has a wide range of technologies from which to choose, ranging from simple bar codes to radio frequency identification technology. In choosing the specific technology, the PM should consider that the technology will change over the life cycle both for the program and the supply chain management information systems using the information. Consequently, it is important the PM take into account the need to plan for and implement an iterative technology refreshment strategy. In addition, since AIT is used by supply and maintenance management information systems it is important that items selected for serialized item management be marked in conformance with MIL STD 129.
- **Need for special handling or supportability factors.** This includes the need for special facilities or packaging, handling, storage, and transportation (PHS&T) considerations. This is usually driven by physical needs (e.g., size, weight, special materials) but can also include eliminating excessive set up and teardown times or the in ability to transport systems without disassembly and reassembly.

5.4. Sustainment in the Life-Cycle Phases

5.4.1. Developing the Support Concept and Establishing Requirements

5.4.1. Developing the Support Concept and Establishing Requirements

Effective sustainment begins with the supportability analysis to form CDD specifications for each supportability parameter to be designed, developed, or procured as proven commercial

technology. It is these analysis-driven supportability parameter specifications, once integrated through systems engineering with all other technical parameters, which drive deployed system operational availability, sustainment effectiveness, and operator ownership affordability. As discussed below, supportability analyses establish supportability performance capability KPP/KSA parameters for Sustainment in the Joint Capabilities Integration and Development System (JCIDS) requirements documentation and are central to the systems engineering process of identifying and refining all system technical performance capabilities.

5.4.1.1. Sustainment in the Joint Capabilities Integration and Development System (JCIDS) Process

Performance-based life-cycle product support implementation begins in the JCIDS process with the exploration of capabilities defined in terms of overall performance and linking sustainment to performance. Every system is acquired to provide a particular set of capabilities in a specific concept of operations, and sustained to an optimal level of readiness. Understanding user needs in terms of performance is an essential initial step in developing a meaningful support strategy because changes to the CONOPS or the sustainment approach may impact the effectiveness, suitability, or cost of the system. Consequently, operational commands and organizations supporting the combatant commanders should be involved in establishing the requirements since they are generally the system users. Their needs should be translated into performance and support metrics to serve as the primary measures of support system performance.

An effective and affordable logistics support program should be represented as a performance capability priority. As discussed in section 1.3, the JCIDS process documents performance capabilities where Warfighters, or their operational user representatives, identify needed supportability and support related performance capabilities parameters (e.g., sustainment metrics, footprint limitations, cost per operating hour, diagnostic effectiveness). Sustainment planning and resource requirements should be mapped to these specific user needs for support related system performance. Further, programs can more easily invest in sustainment features such as condition based maintenance plus (CBM+) and related embedded instrumentation technology, when they are tied to JCIDS performance parameters.

The JCIDS analysis process is composed of a structured methodology that defines capability gaps, capability needs, and approaches to provide those capabilities within a specified functional or operational area. Based on national defense policy and centered on a common joint war fighting construct, the analyses initiate the development of integrated, joint capabilities from a common understanding of existing joint force operations and doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) capabilities and deficiencies. The JCIDS analyses are led by the sponsor and linked into the Life-Cycle Management System at each phase and milestone.

The JCIDS Instruction (CJCS Instruction 3170.01) and Manual require that key considerations for sustainment be addressed early in the analysis as indicated below:

- A Key Performance Parameter for Sustainment has been mandated which treats logistics supportability as a performance capability inherent to the systems design and development
- A Sustainment Key Performance Parameter (Materiel Availability) and two mandatory supporting KSAs (Materiel Reliability and Ownership Cost) are required for all JROC Interest programs involving materiel solutions.
- Logistics supportability becomes an inherent element of operational effectiveness.
- The Capability Development Document and Capability Production Document (CPD) must state the operational and support-related/sustainment performance attributes of a system that provides the desired capability required by the Warfighter -- attributes so significant that they must be verified by testing and evaluation
- The DOTMLPF includes analysis of the entire life cycle, including the sustainment; environment, safety, and occupational health (ESOH); and all human systems integration (HSI) domains.
- The process to identify capability gaps and potential materiel and non-materiel solutions must be supported by a robust analytical process that objectively considers a range of operating, maintenance, sustainment, and acquisition approaches and incorporates innovative practices -- including best commercial practices, HSI, systems engineering (including safety and software engineering), collaborative environments, modeling and simulation, and electronic business solutions.
- The approaches identified should include the broadest possible range of joint possibilities for addressing the capability gaps. For each approach, the range of potential sustainment alternatives must be identified and evaluated as part of determining which approaches are viable.

Initial Capabilities Document (ICD). JCIDS analyses provide the necessary information for the development of the ICD. The lessons learned, cost drivers of current systems, and/or constraints impacting the supportability related design requirements of the planned system, and support system should be documented in the ICD. In addition, the sustainment metrics and the following supportability drivers should be included in the ICD because they guide the acquisition community in refining the concept selected and identify potential constraints on operating and support resource requirements:

- System maintenance/support profiles and use case scenarios;
- Reliability and maintenance rates;
- Support environment and support locations;
- Support and maintenance effectiveness needs; and
- Duration of support.

5.4.1.2. Materiel Solution Analysis Phase Overview

The purpose of this phase is to assess potential materiel solutions and developing a Technology Development Strategy (TDS). This includes identifying and evaluating affordable product support alternatives with their associated requirements to meet the operational requirements and

associated risks. Consequently, in describing the desired performance to meet mission requirements, the sustainment metrics should be defined in addition to the traditional performance design criteria (e.g., speed, lethality). This is because reliability, reduced logistics footprint, and reduced system life-cycle cost are most effectively achieved through inclusion from the beginning of a program and therefore should be addressed in the AoA Plan.

Along with articulating the overall system operational effectiveness objective, this phase is critical for establishing the overarching trade space available to the PM in subsequent phases. User capabilities are examined against technologies, both mature and immature, to determine feasibility and alternatives to fill user needs. Once the requirements have been identified, a gap analysis should be performed to determine the additional capabilities required to implement the support concept and its drivers within the trade space.

5.4.1.3. Activities/Processes

While considered pre-system acquisition, this phase is critical to acquisition program success and achieving materiel readiness because it is the first opportunity to influence systems supportability and affordability by balancing technology opportunities with operational and sustainment requirements. The phase provides the widest latitude for considering requirement alternatives and has the greatest impact on the life-cycle cost. In determining the optimally balanced requirements, emphasis is not only on the reliability and maintainability of potential materiel solutions, but also on assessing cost-effective responsiveness and the relevance of support system and supply chain alternatives.

5.4.1.3.1. Identifying and Evaluating Alternatives

During this phase, various alternatives are analyzed to select the materiel solution and develop the TDS to fill any technology gaps. Figure 5.4.1.3.1.F1 highlights the key activities in identifying and evaluating alternatives and their system sustainment and product support implications. This process is critical because the resulting details guide the acquisition community on refining the concept selected and identifying potential operating and support resource constraints.

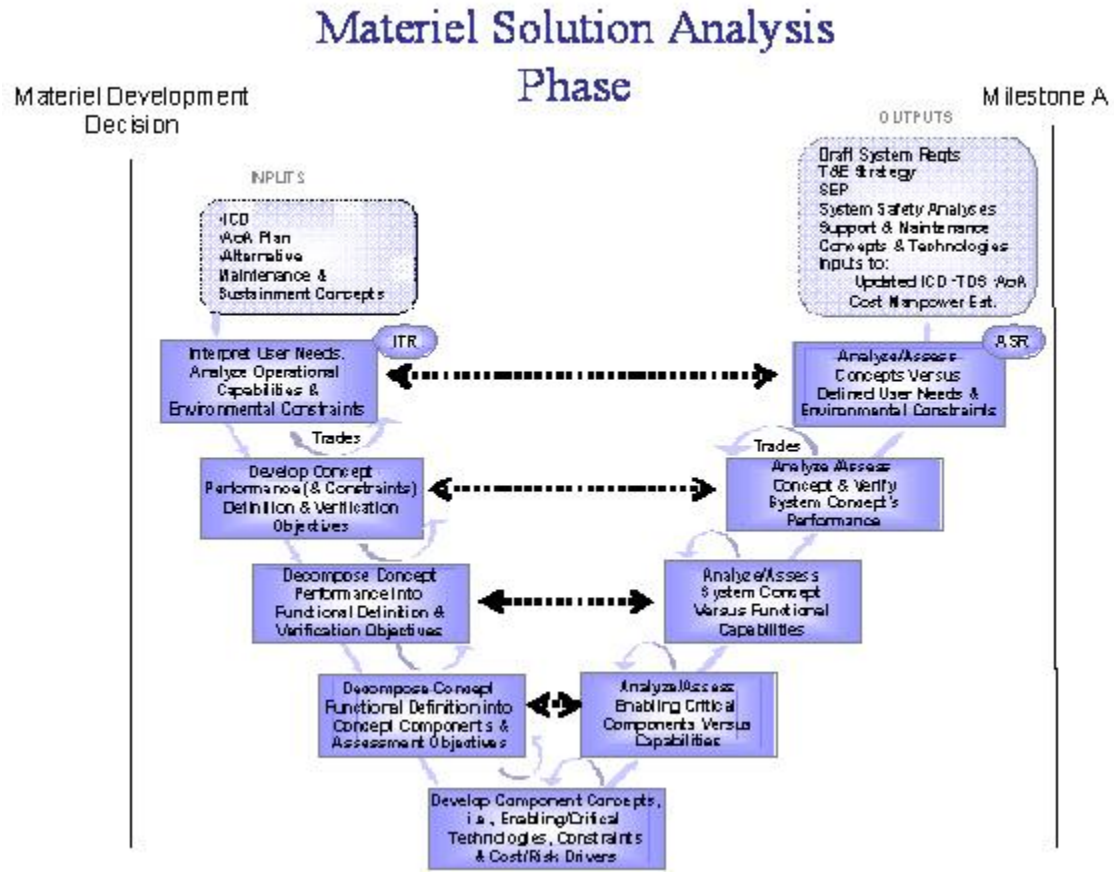


Figure 5.4.1.3.1.F1. System support implications in the Materiel Solution Analysis Phase

Analysis of Alternatives (AoA). The analysis should evaluate the mission effectiveness, operational suitability, and estimated life-cycle cost of alternatives to meet a mission capability in determining the system concept. The AoA team should include functional sustainment performance and associated life-cycle cost analysis expertise to help ensure the AoA assesses the ability of each material alternative candidate to meet and sustain the system's JCIDS performance sustainment capability parameters. It is important that the analysis of alternatives includes alternative maintenance and sustainment concepts consistent with the physical and operational environment of the proposed system. Specific consideration should be given to the associated performance metrics to achieve the required effectiveness goals and the overall ability to accomplish a mission, including the ability to sustain the system. Consequently, during this phase the focus is on determining the system level sustainment metrics and values that provide the balance between mission effectiveness, LCC, logistics footprint, and risk that best represents Warfighter needs. This needs to be done for each system alternative analyzed and for their associated sustainment and maintenance strategies. The strategies must then be broken down to their respective drivers to determine the gaps between what is needed to achieve the mission capability and what is currently achievable. The drivers then become performance-based metrics for sustainment enablers. The gaps indicate risk areas and become candidates for potential

technology development initiatives. Since operational suitability is the degree to which a system can be used and sustained satisfactorily in the field (in war and peace time), consideration should be given to reliability, availability, maintainability, compatibility, transportability, interoperability, sustainment, documentation, and all the HSI domains (Manpower, Personnel, Training, HFE, Environment, Safety, Occupational Health, Survivability, and Habitability).

This analysis should be accomplished by:

- Forecasting the physical and maintenance environment of the proposed system. This should include the projected sustainment demands.
- Using the forecasted environment to assess the functional characteristics of the proposed system, its complexity, and the obstacles and enablers for effective sustainment.
- Assessing the impact of the proposed system on the maintenance capabilities planned for the period in which the system will be introduced.
- Assessing the preliminary manpower and personnel requirements and constraints in both quantity and skill levels.
- Compiling initial information and requirements for the logistics footprint, deployment requirements, and other factors affecting the in-theater operational concept. Even this early Rough Order of Magnitude (ROM) estimates can be performed with comparisons to prior systems or systems of similar capability.
- Developing initial operating and support reliability objectives and their corresponding benefits and resource requirements. This can be done by comparing the performance histories of prior systems or systems of similar capability where feasible for the critical maintenance/sustainment enablers required to achieve the operational requirements.
- Developing ROM life-cycle cost estimates.

Data collected and analyzed during the analysis of alternatives should be retained because it can be useful for subsequent performance-based product support analysis including providing the baseline for logistics footprint and other factors affecting the in-theater operations concept. (See section 3.3.3) As a result, the sustainment related data should be maintained in a manner to make it easy to update program deliverables during subsequent phases, especially prior to milestone decisions.

5.4.1.3.2. Sustainment Metrics

During the Capabilities-Based Assessment (CBA) process, the operational framework and the Combatant Commander's priorities should be defined sufficiently to guide the development of alternative materiel and sustainment solutions. Relevant sustainment criteria and alternatives should be evaluated and addressed in the Initial Capabilities Document in sufficient depth to support the analysis of alternatives and establish the foundation for developing the Sustainment Key Performance Parameter and supporting KSAs in the Capability Development Document and Capability Production Document. At this time, the metrics should be defined and analyzed against the alternatives and a rough plan as to how they will be measured should be developed.

The focus should be on ensuring the metrics are traceable to the ICD, CDD, other JCIDS analysis, or agreement with the user community on the values for each metric and on documented analyses. The analyses should use the most appropriate data sources and include comparisons of corresponding values for analogous existing systems. Where there is a wide difference between values being achieved by today's systems and those needed for the projected environment, further analysis should be done to determine the enabler technologies (e.g., diagnostics, prognostics) required to achieve the sustainment metrics. The analysis should identify the corresponding performance requirements for key enabling technologies. The results should be included in the TDS and Draft CDD.

5.4.1.3.3. Technical Reviews

Many of the actions and subsequent results in this phase are reviewed during technical reviews. The actions and results discussed in this section should be accomplished even if the specific referenced reviews do not occur. The actions and results are tied to the reviews to reflect the relative timeframe in which the actions should be accomplished.

5.4.1.3.3.1. Sustainment Considerations in the Initial Technical Review (ITR)

The ITR ensures a program's alternative materiel solutions are sufficiently defined and technically sound to meet the user's defined needs. The ITR is used to assess the alternatives' viability (cost, schedule and performance risk) and reasonableness given the expected maturity of enabling technologies. Sustainment and product support subject matter experts should:

- Assess the supportability needs and support concept to verify the requisite logistics research, development, test, and programmatic bases for the program reflect the full spectrum of sustainment challenges and risks.
- Ensure historical and prospective sustainment drivers are quantified and the range of uncertainty in these parameters is captured and reflected in the program risks and cost estimates.
- Ensure the cost analysis captures and addresses the key program sustainment and human integration cost drivers for the development, production, operation and support costs.

5.4.1.3.3.2. Sustainment Considerations in the Alternative System Review (ASR)

The ASR helps ensure the preferred system and product support solution satisfies the Initial Capabilities Document. Generally, the review assesses the evaluated alternative systems to ensure that at least one of the alternatives has the potential to be cost effective, affordable, operationally effective and suitable, and can be developed to provide a timely solution at an acceptable level of risk. See section 4.3.1.4.2 for additional information on how the ASR ensures the requirements agree with the customers' needs and expectations.

For this review to be fully effective, the support concept should be addressed as an integral part of the system concept. During the review, the system concept should be assessed with particular attention to understanding the driving requirements for reliability, availability, maintainability, down time, total ownership cost, and the enabling technologies required to meet user requirements. Completion of the ASR should provide:

- An agreement on the support concept to be used as the baseline for subsequent trade studies. The support concept should include the conceptual description, scope, and risk for both the system, as well as any supply chain system/software needs beyond what is currently available.
- The results of any sustainment and support concept trade studies/technical demonstrations to develop the concept or reduce risks.
- Refined thresholds and objectives (initially stated as broad measures of effectiveness). This should include a comprehensive rationale for the preferred solution and the proposed sustainment requirements based on an analysis of alternatives that included cost, schedule, performance (including hardware, human, software), and technology risks.
- Product support constraints to enable integration with the operational and support environments.
- Planning for the Technology Development phase addressing critical sustainment enabling hardware and software to be developed and demonstrated/prototyped, their cost, and critical path drivers. Planning should be based on a comprehensive assessment of the relative risks associated with the preferred support concept including commercial off-the-shelf items in the program. It should emphasize host platform environmental design, diagnostic information integration, and maintenance concept compatibility.
- Sustainment requirements for the draft system requirements document, consistent with technology maturity and the proposed program cost and schedule for the technical baseline and preferred support concept. This should include any commonality, compatibility, interoperability, integration or joint requirements.

5.4.1.4. Materiel Solution Analysis Phase Results/Exit Criteria

The focus of this phase is on identifying the initial concept and any critical product support capability requirements. Affordable operational effectiveness is the overarching sustainment objective that should be considered during the JCIDS process. Implementing the process contained in figure 5.4.1.3.1.F1 results in the preferred system concept and the planning to mature the enabling technologies. The conclusion of this phase produces the initial acquisition strategy (including the sustainment strategy), contractual documents required to continue into the Technology Development Phase and includes the initial support & maintenance concepts as well as LCC and manpower estimates for the system concept.

Table 5.4.1.4.T1 identifies the most critical documents that should incorporate or address sustainment/logistics considerations. Entry documents should be complete when the phase is initiated and include the specific product support issues to be addressed in the phase along with a notional Maintenance & Sustainment Concept of Operations (CONOPS) consistent with the

projected Operational CONOPS. Exit documents are completed or, in the case of the Maintenance & Sustainment CONOPS, updated based on the analysis of alternatives results. The key sustainment elements to be addressed in the next phase should be included in the Acquisition Strategy, the Technology Development Phase RFP, and Source Selection Plan.

Entry Documents:
Initial Capabilities Document
Analysis of Alternatives Plan
Alternative Maintenance & Sustainment Concept of Operations
Exit Documents
Analysis of Alternatives (including Market Research results)
Draft Capability Development Document Technology Development Strategy
Test and Evaluation Strategy
Acquisition Strategy
SEP
Initial Support & Maintenance Concepts

Table 5.4.1.4.T1. Sustainment Considerations in Materiel Solution Analysis

The **Analysis of Alternatives Report** should describe the alternative maintenance and sustainment concepts consistent for each alternative analyzed along with the support capabilities drivers and any gaps. The exit documents should contain the following sustainment related information for the preferred system concept:

- **ICD/Draft Capability Development Document** – the description of the specific enabling technology capabilities required to achieve the drivers and/or to reduce risks in achieving the sustainment metrics values required to meet the operational requirements. The same should be done for each of the corresponding enabling technologies
- **Technology Development Strategy** - the approach for achieving the required enabling sustainment technologies (including design criteria in the Preliminary Design Specification for each of the sustainment drivers). It should also identify the required associated performance metrics and their values.
- **Test and Evaluation Strategy** – the identification of the metrics to be evaluated in subsequent phases and the general approach for evaluating the likely achievement of each
- **Acquisition Strategy** – the overall strategy for achieving the Sustainment Strategy with a focus on how the drivers will be acquired.
- **Initial Support & Maintenance Concepts** – an overview including the supply chain concept and the extent to which the program is taking advantage of existing supply chain processes and maintenance capabilities.

5.4.1.5. Sustainment Considerations in the Materiel Solution Analysis Phase

Use of M&S should be considered to gain an understanding of the dependency and interplay between designed-in capabilities, processes, availability, and life-cycle cost. While at a high level during this phase, each design alternative examined within the operational concept should be considered as to system availability, LCC, and maintenance and sustainment concept drivers. It is important the analysis of alternatives consider the physical and maintenance environment of the proposed systems in the assessment of the alternative system support concepts.

During this phase, support considerations should address the degree to which a system's design and planned logistics resources support its readiness requirements and wartime utilization. This includes consideration of activities and resources (such as fuel) necessary for system operation as well as real world constraints and environment. It also includes all resources that contribute to the overall support cost (e.g., personnel; equipment; technical support data; and maintenance procedures to facilitate the detection, isolation, and timely repair/replacement of system anomalies).

5.4.1.6. Best Practices during the Materiel Solution Analysis Phase

Modeling and simulation combined with LCC analysis are critical best practices and should be included in the AoA Plan. In addition, both should be used as a source selection factor in the Technology Development Phase selection process and to define the desired ranges for the sustainment metrics thresholds and objectives.

5.4.1.6.1. Life-Cycle Cost

During this phase, both acquisition and O&S costs need to be considered in evaluating affordable alternatives. Also during this phase, key sustainment related cost performance criteria, such as O&S cost per operating hour, can be considered in implementing CAIV principles.

Logistics footprint minimization in projecting and sustaining the force is an overarching DoD goal because minimizing the logistical burden a system will place on deployed forces benefits the user, improves deployment time, and can help reduce the LCC. During this phase, footprint metrics appropriate to the system and its operational environment should be analyzed and considered as subsequent KPP, KSA, or design requirements. At a minimum, logistics footprint metrics to meet the concept of operations should be established to be used in baseline trade analyses throughout the life cycle to help impact the design and establish a minimal logistics footprint for the system concept.

5.4.1.6.2. Modeling and Simulation

During this phase M&S supports the requirements determination efforts by analyzing the impact of various alternatives to determine an achievable range of the sustainment metrics values to meet the functional requirements. M&S should be used to assess the alternatives, ensuring all sustainment metrics are considered in parallel and not at the expense of the others. In addition, sensitivity analyses should be used to determine the:

- Optimum mix of key metric values (e.g., LCC and readiness drivers) required to meet the requirements and identify corresponding confidence levels for each of the alternatives
- Impact on sustainment, LCC, and readiness drivers if the supply chain performs at today's performance levels.
- Associated sustainment/maintenance concepts for each of the alternatives to be used as the baseline in subsequent phases

Combining these factors will help identify specific areas where new technology is required to achieve or to reduce risks and increase the probability of achieving the requirements.

5.4.2. Sustainment in the Technology Development Phase

5.4.2.1. Overview

The purpose of this phase is to reduce technology risks (including required sustainment technologies to achieve the needed materiel availability) and determine the technologies to be integrated into the system. The focus is on developing the preliminary design (down to the subsystem/equipment level), reducing integration and manufacturing risk, and, from a sustainment perspective:

- Designing-in the critical supportability aspects to reduce sustainment technology risks and ensuring features (including CBM+ technologies) are incorporated into the system specifications and test plans.
- Developing the initial product support package framework, options, and requirements for the long-term performance-based support concept.

This phase is the most critical for optimizing system sustainment through designed-in criteria to help ensure sustainability. Particular attentions should be paid to reducing the logistics footprint, implementing human systems integration, and designing for support to help ensure life-cycle affordability. Also, during this phase detailed plans for organizing to manage the implementation of the product support package should begin.

The support concept should be defined going into this phase. The phase should be used to define the design-to requirements and to design the product support package. Technology demonstrations and prototyping should be conducted to help determine mature, affordable technologies to be included in the system and support system designs. The demonstrations results coupled with analysis should be used to refine requirements and the LCC estimate, narrow the ranges of all program metrics, and increase confidence the values can be met at an affordable cost.

5.4.2.2. Activities/Processes

This phase is important because cost/schedule/performance/sustainability trade-off analyses linked to demonstrated technologies increase the confidence performance, cost, and schedule thresholds can be achieved. During this phase, the logistics emphasis is on maturing the technologies that enable achievement of supportability objectives, on performing requirements refinement and trade-offs to evaluate the achievable performance given the demonstrated technologies, on refining the supportability objectives, and on identifying any constraints that will limit the system or its supply chain to achieve the operational readiness or mission effectiveness. Figure 5.4.2.2.F1 highlights the key activities.

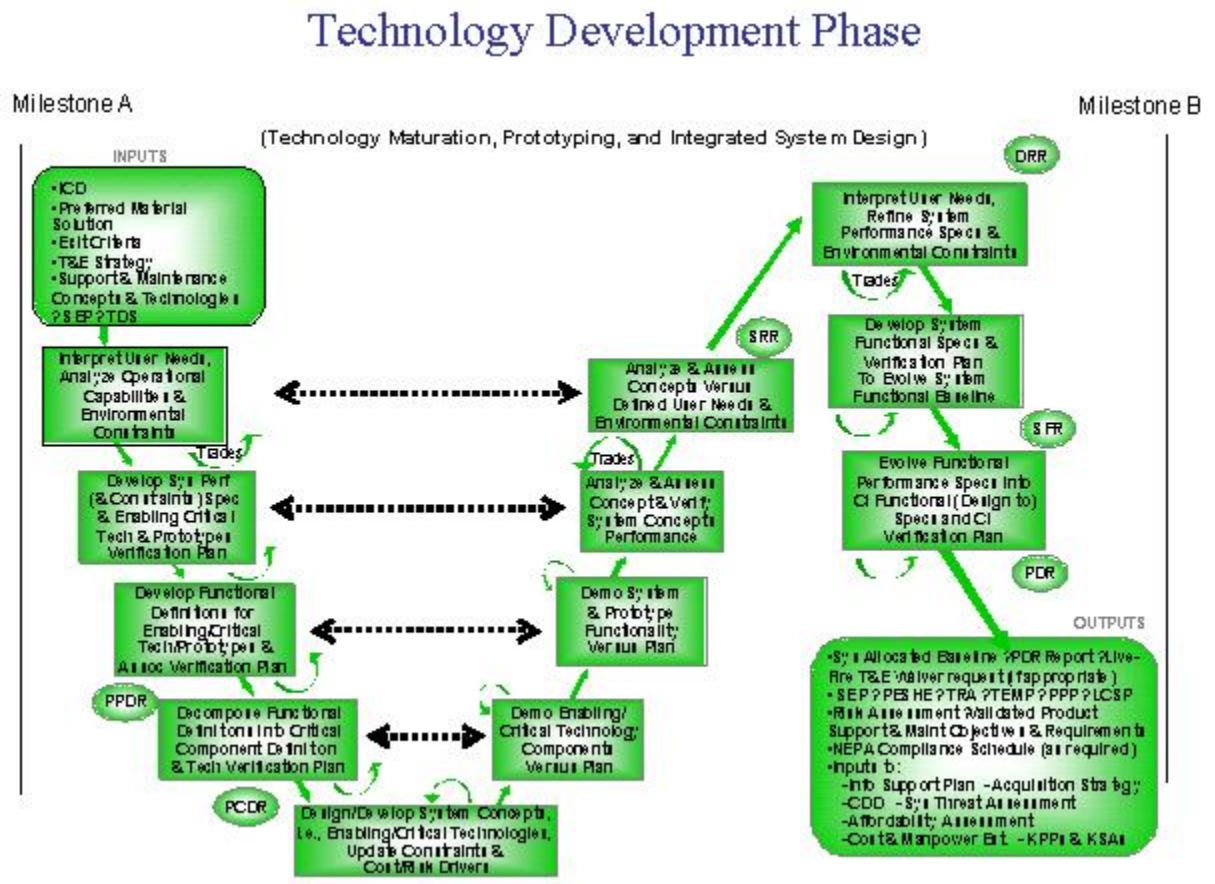


Figure 5.4.2.2.F1. System support implications in the Technology Development Phase

Cost/Schedule/Performance/Sustainment Trade-Offs. In all life-cycle phases, cost, schedule, performance, and sustainability may be traded within the trade space between the objective and the threshold without obtaining Milestone Decision Authority approval. Consequently, it is critical the trade space be established early and be acceptable to the user and acquisition communities. As a result, the operational user and sponsor should be involved with the determination of the trade space and involved in trade-off decisions during this phase. The following are the key steps for establishing the trade space and determining the specific developmental requirements:

- Include sustainment requirements and/or considerations in Advanced Concept Technology Demonstrations, Advanced Technology Demonstrations, and other technology oriented demonstrations and prototyping. The demonstrations should be used to help assess the maturity of available and planned technology required for:
    - The preferred operating and support concepts
    - Achieving the best balance between mission effectiveness, life-cycle cost, logistics footprint, and risk

    - The sustainment performance driver parameters that best represent user needs in achieving operational readiness.
- Forecast the physical and operational environment of the proposed system along with corresponding notional operating and support concepts. The forecast should include consideration of future projections of domestic and foreign facilitation and logistics infrastructure. Specific consideration should be given to the performance-based requirements to achieve the objectives / thresholds for each of the alternatives considered and determining gaps based on technology availability. The gap analysis needs to take into account the complexity and the obstacles to, as well as, the required enablers for effective sustainment likely to be available when the system is deployed considering the current state of the art and likely funding. These gaps should then be used to eliminate alternatives or to determine specific technologies to be developed. It should also form the foundation for a corresponding technology development and verification strategy.
- Perform a market analysis (both public and private) for the needed system and product support capabilities to fill the gaps. The analysis should address the extent and scope of opportunities for using commercial items and processes. It should consider and assess the:
    - Elements of support currently provided (for any legacy systems to be replaced).
    - Current measures used to evaluate support effectiveness.
    - Current effectiveness of required support.
    - Existing support data across the logistics support elements.
    - Existing technologies and associated support that impact the new system
- Develop the functional characteristics and performance specification of the system and its support system based on the best balance between mission performance, life-cycle cost, logistics infrastructure and footprint, and risk. An analysis should be conducted to identify key performance and related support parameters for inclusion in the CDD. The analysis should form the basis of design requirements for subsequent phases and will affect the KPPs/KSAs and the overall capability of the system to perform and endure in the required mission environment. ROM LCC estimates should be developed and included in the analysis results based on the following key elements:
    - Preliminary manpower and personnel requirements estimates. This should also include an assessment of any constraints in both quantity and skill levels and the use of contractor support
    - Operational effectiveness, reliability, maintainability, supportability and interoperability drivers. This should include embedded and external diagnostics, prognostics, and other maintenance enabler technologies that will be required based on suitably mature new design technology. In identifying the drivers and their threshold and objective values, performance histories of similar systems should be examined to determine the feasibility/risks of achieving the required levels and develop a risk mitigation plan. If one has to be developed, the corresponding benefits and resource requirements for each of the drivers should be identified.
    - Logistics footprint metric estimates, deployment requirements, and other factors affecting the in-theater operational concept. This should include the elements the

program will be responsible for and the supply chain performance requirements upon which the program will require to meet operational effectiveness objectives.

Depot Maintenance: During this phase, the following actions are required:

- Finalization in the determination of the organic source of repair to be assigned primary responsibility for maintenance and repair of each system and each sub-system having a core capability requirement.
- Estimate the ROM for the depot-level maintenance workload to be performed at organic facilities for the system and each subsystem.
- Determine the technical data, facility and equipment requirements to ensure the capability to support these workloads.
- Program the resources for the technical data, facilitation, and equipment requirements.
- Summarize the results of these actions in the Acquisition Strategy submitted for Milestone B approval.

5.4.2.2.1. Initial Life-Cycle Sustainment Plan

During this phase, the LCSP documents the maintenance & support concepts based on the results of any technology demonstrations and analyses performed to date. The LCSP further expands on the sustainment strategy and maintenance concept. It should describe the envisioned sustainment capabilities as viewed by the user and major support providers (e.g., the maintainer, supplier and transportation providers). Taking into account the real world constraints and limitations (including "core" requirements, statutory requirements, etc.), it should include:

- The sustainment metrics (including their threshold and objective values).
- A description of the maintenance and support concepts for the major systems within the system. (This high level sustainment concept should include a general description of the support locations and duration including the results of the Core Logistics Analysis and Source of Repair Analysis.)
- A description of the key enablers along with their specific capabilities needed to achieve the operational / system effectiveness requirement.
- The basic strategy that will be used to achieve the program with the associated budget.

See figure 5.4.2.2.1.F1 for notional LCSP focus areas for this phase. As the design evolves, the LCSP should also expand and by the SRR (or when the System Specification has been developed) it should also contain the following information:

- **Supportability Design Characteristics** – Describes the key design characteristics included in the contract and how demonstrated performance is tied to incentives. In addition to the design characteristics, it should also include specific information on:
    - How reliability & maintainability and sustainment metric performance will be measured during development/testing including the expected maturity curves.

  - The subsystems with diagnostics and/or prognostics features and how the status/projected status along with the effect on mission capabilities will be conveyed to the operator and maintainers.
- **Supportability Analysis Process** – Addresses the processes to establish the requirements for all logistic elements and keep them aligned/balanced as the design and supply chain evolve. This should include at a minimum how the following are being used to establish the requirements:
  - Maintenance planning analysis results (with specific emphasis on how RCM is being used to determine the preventative maintenance and corrosion prevention & control requirements) relative to the best level to perform maintenance to achieve the materiel availability requirement and the associated KSAs.
  - Training and HSI requirements, including the training requirements/objectives (for both operator and maintenance training) relative to training courses, materials, and training equipment to enable personnel to effectively perform tasks supporting the CONOPS and the maintenance concept. The requirements for specific training strategies to be used to meet the Sustainment KPP, such as distance learning should also be addressed.
  - The Source of Repair Analysis (SORA) and DSOR Analysis should include describing how Title 10 Requirements, such as Core and 50/50 are being met.

1. Current Program Description – Describes how sustainment considerations are being implemented in the program

- **1.1 Sustainment and Maintenance Concepts**
- **1.2 Sustainment Acquisition Strategy**
- **1.3 Sustainment Funding/Budget** – RDT&E categories should be broken out by outcome/product for sustainment efforts. Procurement and O&M categories should be shown to provide stakeholders a feel for the resources planned to support the program

	Prior	Current Yr	FY+1	FY+2	FY+3	FY+4	FY+5	FY+6	Pgm Completion
RDT&E Rqd									
RDT&E Budget									
Procurement Rqd									
Procurement Budget									
O&M Rqd									
O&M Budget									
Milcon Rqd									
Milcon Budget									

- **1.4 Stakeholders**

2. Program Performance/System Indicators & Requirements – Describes key sustainment metrics. In addition to the metric and its definition, this section should include the goal & threshold.

- **2.1 Materiel Availability**
- **2.2 Materiel Reliability**
- **2.3 Mean Down Time**
- **2.4 Ownership Cost**
- **2.5 Additional sustainment enabler metrics**

Metric	Objective	Threshold	Definition	Verification Method
Materiel Availability				
Materiel Reliability				
Mean Down Time				
Ownership Cost				
Others				

3. Sustainment Implementation Plan

- **3.1 Supportability Design Characteristics** – Describes the key requirements included in the design specifications.
- **3.2 Supportability Analysis Process** – Describes the processes included in the Systems Engineering Plan being used to establish and keep the product support elements in balance in achieving the sustainment metrics.
- **3.3 Product Support Package** – Describes the plan for fielding the PSP
- **3.4 Sustaining the Weapon System** – Describes the systems engineering and management strategies to sustain the metrics including how ranges and triggers will be used.

4. Program Schedule – Shows major sustainment actions/events

5. Special Interest Items – Describes any additional information on key technologies, initiatives or enablers the program is using

Figure 5.4.2.2.1.F1. Notional Initial Life-Cycle Sustainment Plan Focus

- **Fielding the Product Support Package** – Describes the approach for fielding the product support package, including the major steps in developing and fielding each logistics element describing who is doing what, where and when with the associated budgets described in the Funding/Budget section. There is no specific format or breakdown required and the level of detail will vary depending on the extent to which

outcome based contracts are used - but the following are major categories that should be addressed:

- **Maintenance Plan and Requirements** – Describes the management approach for developing and implementing the maintenance requirements. The management aspects should include the logistics management structure being used (e.g., Maintenance Planners, Corrosion Prevention Advisory Team) and how they are integrated with the program's planning, systems engineering, and configuration management structures. It should also address the management documents being used (e.g., Corrosion Plan addressing the Corrosion Prevention and Control Planning Guidebook guidelines) and the training and certification required for the personnel involved with determining the maintenance requirements. The analytical aspects should describe the process used to determine the best level and schedule to perform preventative maintenance to achieve the sustainment metrics (e.g., RCM process complies with the SAE JA1011 standard), the resultant logistic requirements, and the process for validating the reliability & sustainability contract requirements have been met. It should also include a description of the tools/processes/data bases to collect, store and analyze actual performance and project how the data will mature (from initial tests until after the program is fully operational).
- **Product Support Package Elements** – an overview of each of the following elements should be included:
  - Technical Documentation (Paper Based and/or Electronic-Interactive)
  - Test/Support & Calibration Equipment
  - Manpower & Training/Computer Based Training.
  - Supply Support (including Spare/Repair Parts)
  - Packaging, Handling, Storage, & Transportation
  - Facilities
  - Computer Resources Support

5.4.2.2.2. Maintenance & Sustainment Strategy Development

The maintenance & sustainment strategy should be refined from the projected system's reliability and the preliminary sustainment concept of operations to meet the operational requirement in the planned environment. They are then used to determine the supply chain performance requirements, along with the key enabling features needed to implement the strategy. These enablers can range from system design features (e.g. condition based maintenance) to supply chain features (e.g., rapid distribution of tailored support packages, just in time training / distance support, total asset visibility anywhere in the support chain, dedicated rapid response support teams analyzing real time data). The details should be described in sufficient detail to provide assurance that risks are understood and the gaps can be filled.

Core logistics and repair sources are critical elements in establishing appropriate repair and support capability. New and emerging systems may lack mature data at this stage, but by using data from similar current systems and subsystems, planning for a sustainment strategy can

evolve. Key activities should include establishing the baseline for trade studies by identifying notional maintenance levels and activities for major subsystems, taking into account system/subsystems with a core capability.

The gaps between the current state of the art and current sustainment/maintenance capabilities versus what is required (along with the risk) should be used to identify technologies needing to be developed and demonstrated in subsequent phases. They should also be used in developing the implementation plan for proceeding with the best value alternative and summarized in the LCSP. The following are key considerations in developing the performance/cost/schedule/ sustainment and risk tradeoff analysis:

- The relative cost vs. benefits of different support strategies.
- The methods and rationale used to quantify benefits and costs.
- Data required to support and justify the best value support strategy.
- Sensitivity of the data to change.
- Analysis and classification of risks.

Core Capability Planning and Analysis. The requirement for determining core requirements and applying this methodology extends to all weapon systems and equipment operated by each DoD Component, regardless of where depot-level maintenance is actually performed (DoDI 4151.20, "Depot Maintenance Core Capabilities Determination Process,"). The following depot maintenance core capability requirements determination methodology is used to determine essential DoD depot maintenance capability requirements for each DoD Component, and the workloads needed to sustain those capabilities.

- Programs requiring a core capability/DSOR decision shall be identified by the managing Service Acquisition Program Manager (PM) (or Joint Program Office (JPO) in the case of Joint Service acquisitions) to the Service organization(s) responsible for depot-level maintenance management (hereafter referred to as MMOs). Joint programs, and those having depot-level maintenance inter-servicing potential, shall be identified by each DoD Component MMO in conjunction with the PM/JPO.
- The identification of the need for a core determination will occur at least 180 days prior to the Acquisition Milestone B decision need date. For systems entering the acquisition process after Milestone B, identification will occur immediately following the acquisition approval.
- It is the responsibility of the Acquisition Program Manager (PM) (or Joint Program Office (JPO)) in conjunction with the DoD component that owns the depot-level maintenance assets to ascertain the potential need for establishing an organic core capability requirement by addressing, at a minimum, the following questions. Other considerations may be applied, as appropriate:
- Is the system replacing a system having a core capability requirement at either the system or the subsystem level? If the answer is "Yes" then it can be assumed that this system and its subsystems will require the same core capability requirements as the system being replaced, adjusted for known inventory and workload differences.

- If not, will the system be used or is it planned to be used in support of a JCS contingency scenario? If the answer is "Yes" then Section 2464 of Title 10, United States Code requirements for the establishment of organic core capability apply.
- If the answer to either question is 'yes', an initial core capability requirement determination analysis must be conducted and candidate Depot Source of Repair (DSOR) depot-level maintenance facilities identified by the DoD Component(s).
- After core requirements have been determined, the PM/JPO shall take appropriate steps to assure that the requirements for the establishment of organic capability are included in all product support acquisition requirements (e.g. need for tech data, peculiar support equipment, facilities and/or Public Private Partnership).
- While not part of the core determination process it is at this stage that any requirements to assign a portion of the proposed workload to an organic depot to provide reasonable assurance of future compliance with the 50/50 requirements be identified and provided by the DoD Component(s) MMOs to the PM/JPO along with justification and documentation for use in designing the product support strategy.

5.4.2.2.3. Technical Reviews in Technology Development

Many of the actions and subsequent results in this phase are reviewed during technical reviews. The actions and results discussed in this section should be accomplished even if the specific referenced reviews do not occur. The actions and results are tied to the reviews to reflect the relative timeframe in which they should be accomplished. In the new life-cycle model, competitive prototypes are now used and each may undergo a Prototype Preliminary Design Review (P-PDR) and a Prototype Critical Design Review (P-CDR). Sections 5.4.2.2.3.3 and 5.4.3.2.2.1 provide information for the types of sustainment considerations during these reviews.

5.4.2.2.3.1. Sustainment Considerations in the System Requirements Review (SRR)

The SRR is conducted to ascertain the results of the prototyping and demonstrations relative to the system technical requirements. It determines the direction and progress of the systems engineering effort and the degree of convergence upon a balanced and complete system baseline. (See section 4.3.2.4.2.1 for additional information.) The purpose is to ensure all system requirements (performance requirements and sustainment requirements) derived from the Initial Capabilities Document (ICD) or draft CDD are defined, consistent and achievable within cost, schedule and any other constraints. Generally the SRR assesses the prototyping results with respect to the system requirements captured in the system specification and support strategy to ensure they are consistent with the system and support solution as well as available technologies.

The SRR is important in understanding the performance requirements, cost, and scheduling impacts on the system and its support concept. During the SRR, the systems requirements are evaluated to determine whether they are fully defined and consistent with a demonstrated mature technology solution. A successful review is predicated on determining the system and support

element requirements are based on available technology, a sustainable support concept, and program resources (e.g., funding, staffing, processes and schedule). Logistics and product support subject matter experts should participate to ensure the critical sustainment system and support elements enabler technologies required to implement the support strategy and achieve the needed materiel availability are included in the planning and performance specifications. Understanding and accepting the program risk inherent in the system specification, Systems Engineering Plan and Life-Cycle Sustainment Plan is key to a successful review. The SRR should provide:

- An approved system performance specification with achievable system, supportability, human systems integration, and sustainment enabler requirements which satisfy and are traceable to the ICD or draft CDD and support concept.
- A preliminary allocation of system requirements to hardware, human, and software subsystems. The system sustainment requirements should be sufficiently detailed and understood to enable system functional definition and functional decomposition.
- Demonstration that critical sustainment system and support element enabler technologies required to implement the support strategy and achieve the needed materiel availability are sufficiently mature to enable low risk entry into development.
- Approved support and sustainment concepts with the corresponding metrics.
- A preliminary Cost Analysis Requirements Description consistent with the approved system performance specification and sustainment concept.

5.4.2.2.3.2. Sustainment Considerations in the System Functional Review (SFR)

The SFR ensures the system functional baseline has a reasonable expectation of satisfying the CDD requirements within the allocated budget and schedule. A critical SFR aspect is the development of representative operational and product support use cases for the system. System performance and the anticipated functional requirements for operations, maintenance and sustainment are assigned to sub-systems and support systems hardware and support systems hardware & software after analysis of the operational and support environments. The SFR determines whether the system's functional definition is fully decomposed to its lowest level forming the functional baseline, and that IPTs are prepared to start preliminary design. Additional information for this review can be found in section 4.3.2.4.2.2.

Product support IPT members as well as independent supportability and sustainment subject matter experts should participate in the review to ensure the system functionality is consistent with the supportability requirements and the support strategy contained in the evolving Life-Cycle Sustainment Plan (LCSP). This involves:

- Addressing the supportability requirements to support the CDD and the supportability functionality as defined in the functional baseline ensuring adequate processes for achieving the sustainment metrics are in place.

- Defining the detailed support concept functionality requirements for system and subsystem elements to ensure system functional requirements are sufficiently detailed and understood to enable system design supportability analyses to proceed.
- Ensuring program sustainment development efforts (including system and software critical path drivers), with corresponding schedules, are included in LCSP updates.
- Ensuring the updated Cost Analysis Requirements Description (CARD) (or a CARD-like document) based on the system functional baseline, captures the key program sustainment cost drivers, development costs, production costs, and operation & support costs for all aspects of sustainment and human system integration.

5.4.2.2.3.3. Sustainment Considerations in the Preliminary Design Review (PDR)

The PDR helps ensure the system's allocated baseline and its associated support system have a reasonable expectation of satisfying the CDD requirements within the allocated budget, staffing, and schedule and have an acceptable risk level. Details can be found in section 4.3.2.4.2.3 but in summary the PDR assesses the preliminary design captured in the preliminary subsystem product specifications for each configuration item (hardware and software) and ensures each function, in the functional baseline, has been allocated to one or more system configuration items. The PDR evaluates the subsystem requirements to determine whether they correctly implement all system requirements allocated to the subsystem. The Integrated Product Team (IPT) should review the results of peer reviews of requirements, preliminary design documentation (including Interface Control Documents) along with the plans for development and testing for both system performance and supportability aspects to ensure the system is ready to proceed into detailed design and test procedure development.

Product support IPT members, as well as independent supportability and sustainment subject matter experts, should participate in the review to ensure the supportability requirements and the support strategy contained in the Life-Cycle Sustainment Plan (LCSP) are consistent with the evolving design. This involves:

- Addressing the supportability requirements to support the CDD and ensuring the supportability functionality are allocated to each system or subsystem and they can be achieved within the budgets and schedule. This includes ensuring the Failure Mode Effects and Criticality Analysis, Maintainability Analysis, and Reliability Centered Maintenance Analysis results have been factored into the allocated requirements, preliminary design, and risk assessment. In addition to ensuring adequate processes for achieving the sustainment metrics are in place, this includes ensuring the HSI design factors have been reviewed and included in the overall system design.
- Setting the allocated baseline for any system and/or major subsystem product support package elements. This includes defining the detailed support concept functionality requirements for subsystem product support package elements to ensure system functional requirements are sufficiently detailed and understood to enable more detailed supportability analyses to proceed.

- Defining the test success criteria for development testing and operational testing (for both operationally effective and suitable) requirements and the general test approach for key sustainment enablers or drivers.
- Ensuring program sustainment development efforts (including system and software critical path drivers with corresponding schedules) are included in LCSP updates.
- Ensuring the updated Cost Analysis Requirements Description (CARD) (or a CARD-like document) based on the system allocated baseline, captures the key program sustainment cost drivers, development costs, production costs, and operation & support costs for all aspects of sustainment and HSI.

5.4.2.2.3.4. Sustainment Considerations in the Technology Readiness Assessment (TRA)

The TRA is a metrics based process that assesses the maturity of critical technology elements conducted concurrently with other technical reviews. From a sustainment perspective, the process should be used for assessing risk and the adequacy of technology maturation planning when the support concept or sustainment drivers depend on specific new or novel technologies to meet system threshold requirements in development, production, or operation. If a key enabler or sustainment driver (e.g., reliability, turn around time) does not meet required performance levels or significant performance advances is required over what is currently achieved with existing technology, then a Critical Technology Element Maturation Plan should be developed, explaining in detail how the performance level will be reached. See section 4.3.2.4.2.4 for additional information on how the TRA highlights critical technologies (including sustainment technologies) and other potential technology risk areas requiring attention.

5.4.2.2.3.5. Sustainment Considerations in the Integrated Baseline Reviews (IBR)

IBRs are used throughout the program whenever earned value management is used. IBRs establish a mutual understanding of the project performance measurement baseline. While they have a business focus, IBRs can also be useful in ensuring sustainment is considered in the acquisition process when the efforts required to achieve the Sustainment KPP, KSAs and any other key sustainment enabler metrics are included in the reviews. These reviews and resultant understanding also provide for a plan of action to evaluate the risks inherent in the program measurement baseline and the management processes during project execution. Additional information can be found in sections 4.3.3.4.1 and 11.3.1.3.

5.4.2.3. Technology Development Phase Results/Exit Criteria

The focus of this phase is on reducing risk and defining achievable performance and sustainment requirements. This begins with the analysis of alternatives that include examining alternative operating and system support concepts, with specific consideration of performance-based requirements. Success is demonstrated by identifying key performance and related sustainment

metrics (with their basis) as design requirements that affect the overall capability of the system to perform and endure in the required mission environment. (In addition to the Sustainment KPP/KSAs, the metrics can include other supportability, maintainability, interoperability, manpower or footprint measures.) Implementing the process contained in figure 5.4.2.2.F1 produces the refined supportability objectives and, in some cases, anticipated constraints based on the technology assessments. The conclusion of this phase results in the contractual documents required to continue (including the related sustainment requirements and actions) and updated system baseline support & maintenance concepts, LCC, and manpower estimates.

Table 5.4.2.3.T1 identifies the most critical documents that should incorporate or address sustainment/logistics considerations. The key sustainment elements to be addressed in the next phase should be included in the Acquisition Strategy and the materiel availability enabler requirements should be included in the Engineering and Manufacturing System Development RFP as well as the Source Selection Plan. The exit documents from this phase should focus on the materiel availability driver metrics (including drivers for the enablers) and the baseline support strategy. They should also contain the following sustainment related information:

Entry Documents:
Analysis of Alternatives
Technology Development Strategy – Draft Capability Development Document (including sustainment technology issues)
Test and Evaluation Strategy
Initial Support & Maintenance Concepts
Support strategy
Exit Documents:
Analysis of Alternatives (including Market Research results)
System Performance Specification
Capability Development Document
Preliminary Design Review Results
Test and Evaluation Master Plan (TEMP)
Information Support Plan
Acquisition Strategy
Cooperative Opportunities
Core Logistics Analysis/Source of Repair Analysis
Industrial Capabilities
Life-Cycle Sustainment Plan
Life-Cycle Cost Estimate and Manpower Estimate
Preliminary Maintenance Plans

Acquisition Program Baseline (APB)
Affordability Assessment (including DoD Component Cost Analysis & ICE)

Table 5.4.2.3.T1. Sustainment Considerations in Technology Development

- **AoA** - the sustainment driver metrics and product support strategies for each alternative considered along with any gaps and major assumptions
- **System Performance Specification** - objectives and thresholds for the sustainment driver metrics including the corresponding enabler drivers
- **CDD** - the information necessary to deliver an affordable and supportable capability using mature technology. The following sustainment drivers information should be included:
    - System maintenance/support profiles and use case scenarios
    - The corresponding support and maintenance effectiveness measures
    - Description of the specific capabilities required to achieve the support concept and/or to reduce risks in achieving the values required to meet the operational requirements. It should include metrics for each of the key enabling technologies (e.g., reliability/ maintenance rates, diagnostics/prognostics effectiveness measures)
- Preliminary Design Review Results – the description and status of the sustainment driver design features
- Technology Readiness Assessment - approach for achieving the required enabling sustainment technologies (including design criteria for each of the drivers in the preliminary system design specification) (see section 4.3.2.4.2.4)
- Test and Evaluation Master Plan (TEMP) – identification of the metrics and enabling/driver technologies to be evaluated in subsequent phases, the approach for evaluating them, and test points (see section 9.6.2)
- Data Management Strategy – the long term strategy integrating data requirements across all functional disciplines.
- Information Support Plan – plan for acquiring and managing the data required to execute the support concept in the operational environment (see section 7.3.6)
- Acquisition Strategy – containing the LCSP executive summary
- Life-Cycle Sustainment Plan (LCSP) – summary of the maintenance & sustainment concepts including the support locations and duration. It should focus on the support strategy including the contracting strategy to acquire the major elements of the support concept and the specific incentives being used to help achieve the sustainment drivers and enablers
- Life-Cycle Cost Estimate and Manpower Estimate – the major assumptions and values being used for the sustainment drivers and enablers (see Chapters 3 and 6) It should also include the confidence level of the values being achieved
- Acquisition Program Baseline (APB) – description of the sustainment metrics, criteria, and logistics funding requirements (see section 2.1.1)

- Affordability Assessment – an assessment based on the likelihood of the key sustainment metrics being achieved (also see section 3.2.2)

5.4.2.4. Sustainment Considerations in the Technology Development Phase

During this phase, the focus should be on refining the threshold and objective range value estimate for each sustainment metric based on more detailed analysis identifying the technical capabilities, risks, and limitations of the alternative concepts and design options. Analysis should also be performed to identify the impacts the sustainment metrics will have on mission success and materiel availability. The key enabling requirements to achieve the sustainment metrics should be allocated to the major system level and included in the system specification. Even this early it is important to establish the reliability requirements and assess the extent to which the system will likely meet the requirements. Consequently, the reliability of the technology or system should be included in the technology readiness assessments.

Detailed plans for monitoring, collecting and validating key metrics should be established to provide empirical data to evaluate technical performance, system maturity, and the projected logistics burden. Detailed test criteria should be developed for each metric (including any key dependent enabling technologies) to provide information about risk and risk mitigation as the development and testing continue. The test strategy/requirements to provide data and analysis support to the decision process should be documented in the TEMP.

5.4.2.5. Best Practices during the Technology Development Phase

M&S combined with LCC analysis are important best practices to help assess the success in reducing program risk. In addition, both should be used in the Engineering & Manufacturing Development Phase source selection process and to define the sustainment objectives and thresholds to be placed on contract. The data used for the assessments and analysis (including the projected sustainment demand) should be complied and saved for analyses in subsequent phases.

5.4.2.5.1. Supportability Analysis

During this phase, supportability analysis focuses on the technology trade-offs. As indicated in figure 5.4.2.5.1.F1, the analysis process is iterative. They are re-run as required as the design is refined. Trade-off impacts are identified and evaluated to ensure the selection of a system concept that not only delivers system performance, but also achieves supportability, interoperability and system affordability objectives. The supportability analysis goal within this phase is to establish affordable and obtainable thresholds and objectives to achieve the user requirements in the projected environment within the Concept of Operations.

The analyses are iterative, evolving and expanding as more specific design and other technical information on the actual equipment is identified. While the focus is high level for the system at

the beginning of this phase, it should also consider requirements for key enablers in terms of "what is required" vice "how it is accomplished". As the phase progresses, the analysis should determine the relative cost vs. benefits of different support strategies (including potential source of support decisions). The impact and value of performance/cost/schedule/sustainment trade-offs based on the preliminary design should continue expanding to the lowest level of the work break down structure as the design evolves across this and subsequent life-cycle phases.

A complete supportability analysis should be performed for any parts of the system for which the government is going to provide the product support package vice using a contracted approach with materiel availability as the performance measure. Figure 5.4.2.5.1.F1 shows the key system reliability, maintainability and supportability system engineering processes. The affordable system operationally effectiveness analysis process coupled, with available tools and opportunities - such as modeling and simulation, performance testing, supportability testing/demonstration, technical data validation, and maintenance assessments - should be proactively applied and integrated with the systems engineering process. For example, system requirements can be used to develop a system reliability/availability block diagram as a basis for modeling and analysis. This approach can identify opportunities for targeted system redundancy, ease of reconfiguration, and derating, etc., and can thereby enhance system level reliability and availability. In addition, reliability, maintainability (BIT/prognostics), and supportability/ logistics demonstrations can provide the data to assess achievement of RAM requirements.

The level of detail performed by the government team will vary by the extent to which performance-based product support contract is used but that will not impact the general process, including the program major events. As a result, the supportability analysis process should take advantage and be an integral part of the major engineering events and processes, including but not limited to the System Requirements Review (SRR) and Preliminary Design Review (PDR).

As illustrated in Figure 5.4.2.5.1.F1, a FMECA helps identify the ways in which systems can fail, performance consequences, and serve as basis in the identification of Critical Safety Items as well as potential areas for preventative maintenance for the system. When conducted in a timely fashion, the FMECA can be used to support trade-offs between performance and life-cycle costs to drive design improvements. A Fault Tree Analysis (FTA) assesses the safety-critical functions within the system's architecture and design. A Maintainability Analysis and Prediction (MAP) assesses the maintenance aspects of the system's architecture, including maintenance times and resources. This analysis identifies strategic opportunities for focused diagnostics, prognostics, and performance monitoring/fault localization, leading to reduced system maintenance times and cost drivers. A level of repair analysis optimally allocates maintenance functions for maximum affordability and materiel availability.

Once FMECA, FTA, and MAP are completed and system design has been established, RCM analysis develops a focused, cost-effective system preventive maintenance program. RCM uses a system based methodical approach to determine causes of failure, failure consequences, and a logic tree analysis to identify the most applicable and effective maintenance task(s) to prevent failure, if possible. RCM also provides rules for determining evidence of need for condition

based maintenance to perform maintenance only upon evidence of need. (DoDI 4151.22, Enclosure 3)

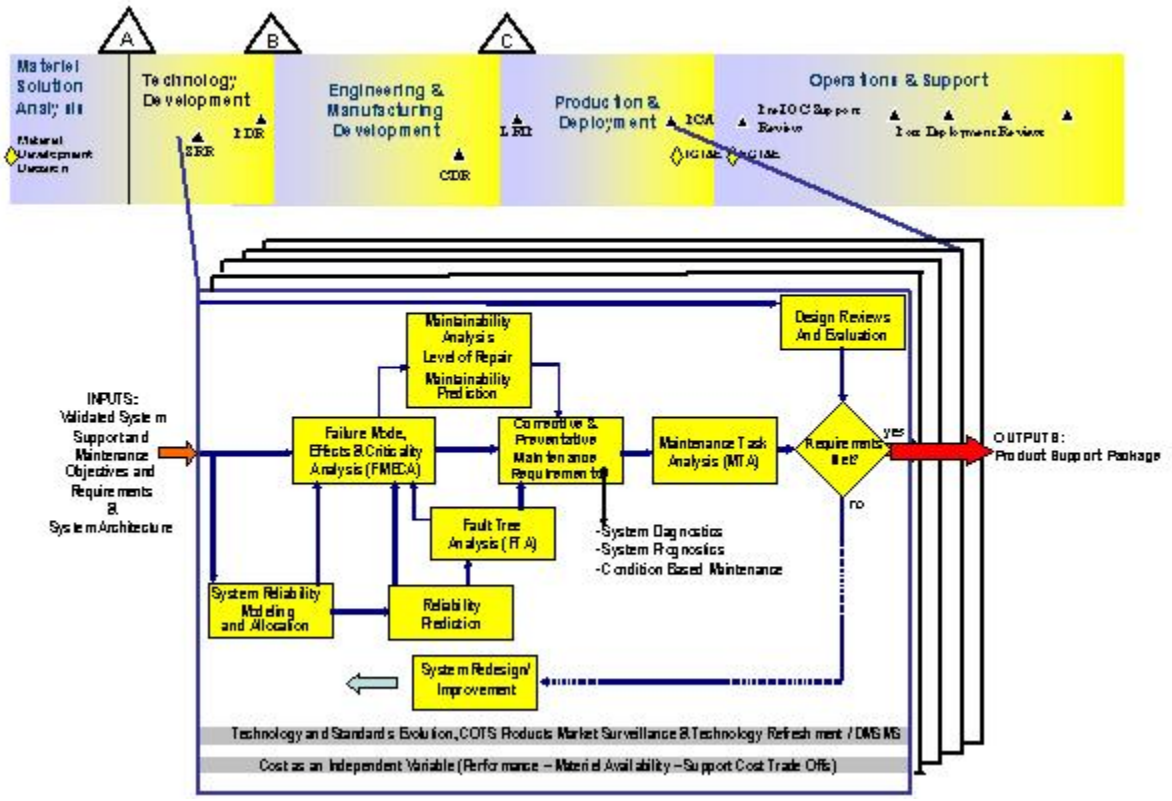


Figure 5.4.2.5.1.F1. Supportability Analysis During Design

A maintenance task analysis identifies detailed logistics and support resource requirements to sustain system readiness. Appropriate use of proactive maintenance technologies embodied in diagnostics and prognostics pays system dividends. Integrating on-board and off-board monitoring, testing, data collection, and analysis capabilities can significantly enhance system maintainability and overall supportability. Typically, practices here include enhanced prognosis/diagnosis techniques, failure trend analysis, electronic portable or point-of-maintenance aids, corrosion mitigation, serial item management, automatic identification technology, and data driven interactive maintenance training. Ultimately, these practices can increase materiel availability and readiness at a reduced cost throughout the life cycle.

The activities shown in figure 5.4.2.5.1.F1 are not necessarily carried out in a linear progression. Design increments and the continuous assessment of test results and in-service system performance will identify needs for system improvements to enhance reliability, maintainability, overcome obsolescence, corrosion, or other sustainment needs.

Risk Assessments. Risk assessments should be performed to identify and develop design trade-off that mitigates risk. Technology risk considerations should receive intensive consideration as the system concept is developed. Maximum use of low-to-medium risk technology, as indicated in Figure 5.4.2.5.1.F2, provides the greatest opportunity to hold to program cost, schedule and performance requirements. Medium-to-high risk technologies should be thoroughly justified and risk mitigation efforts resourced. Use of high-risk technologies should be avoided and be a critical factor in choosing an incremental acquisition strategy.

Once the preferred system, system support concepts and enabling technologies are selected, case scenarios reflecting system support, maintenance, and logistics are refined. These scenarios identify significant system support, maintenance, and logistic requirements and objectives. These are compared to the Sustainment KPP/KSA threshold and objective and expanded in depth as the hardware design matures and the process is iterated until an affordable systems operational effective solution is achieved.

Technology Maturity	Technology Description
Low Risk	Existing Mature Technologies
Medium Risk	Maturing Technologies; New Applications of Mature Technologies
High Risk	Immature Technologies; New Combinations of Maturing Technologies

Figure 5.4.2.5.1.F2. Technology Risk Considerations

5.4.2.5.2. Modeling and Simulation

M&S should be used to refine sustainment objectives (this includes the Sustainment KPP and KSAs as well as any other LCC or readiness driver metrics) and identify any constraints based on technology assessments. The technology demonstration results should be modeled to project likely capabilities and the associated confidence levels that enabling technologies will be achievable in the operational environment. It should also be used to develop initial/notional system level product sustainment strategy and maintenance concepts for major sub systems. All of these elements will be used to project the mature Sustainment KPP/KSA values and their associated confidence levels they will be met within the CONOPS.

As the design evolves, modeling and simulation can be used to help keep the logistics elements in balance between and within system hardware elements. This is done by allocating the sustainment, LCC or readiness driver metrics to specific subsystems and equipments. These requirements are then used to develop the specific system level support strategies and maintenance plans along with their design-to requirements for both the system and its logistic

support system. Modeling at this level of detail provides more creditability especially relative to the following efforts important in this phase:

- Analyzing the impact of proposed budget alternatives on the Sustainment KPP/KSAs (as well as mission effectiveness).
- Assessing the alternatives affecting the design and deployment of both the end item and its support system to ensure all metrics and their drivers are considered in parallel and not at the expense of the others.
- Anticipating and resolving potential problems by taking use data and user feedback for similar equipments and/or sustainment strategies.

5.4.3. Sustainment in the Engineering and Manufacturing Development (EMD) Phase

5.4.3.1. Overview

The purpose of this phase is to develop a detailed integrated design and ensure producibility and operational supportability. The focus is on producing detailed manufacturing designs, not solving a myriad of technical issues. Prototyping and analysis should have been applied prior to this phase to discover and resolve issues to ensure the design is based on a mature technology and is achievable within cost, schedule and sustainment constraints. From a sustainment perspective this means paying particular attention to reducing the logistics footprint; implementing human systems integration; designing for supportability; and ensuring affordability, integration with the supply chain, interoperability, and safety. All of these factors are used to refine the performance-based support concept and strategy, with the associated requirements, and to identify potential support providers.

5.4.3.2. Activities/Processes

During this phase, the focus is on developing the requirements for the long-term performance-based support concept and the initial product support package. In accomplishing this, life-cycle management documents and analyses are refined as a result of the detailed design process, iterative systems engineering analyses and developmental test results. Figure 5.4.3.2.F1 highlights the key activities to be managed by the organizations put into place to implement the program. During this phase, the critical sustainment metrics are also refined and incentives developed for eventual performance-based support contracts and/or performance-based agreements. Stakeholders (including potential support providers) are identified and included in Integrated Product/Process Team (IPT) processes to build an early understanding of and buy-in for sustainment requirements and objectives. Also during this phase, the support concept is refined and potential support providers are identified. Incentives to design for support and to design a cost-effective support concept can, and should, be linked to the support strategy. Identification and involvement of the potential support providers and integrator early during these efforts is essential for program success.

Supportability Analysis. Supportability analysis, modeling and simulation, and life-cycle costing should be applied and integrated with the systems engineering process in increasing levels of detail to determine the relative cost vs. benefits of different support and maintenance strategies; the impact and value of performance/cost/schedule/sustainment trade-offs; and to create the data required to support and justify the support strategy. During this phase, data will be

compiled, refined, and analyzed consistent with acquisition policy and Defense Acquisition Board (DAB) requirements to develop and document a best value long term support strategy. The assessment process determines the right mix between organic and commercial performance-based support and should consider all requirements (including statutory) when determining the best value long term sustainment approach to optimize readiness while minimizing cost. The programs should use accepted decision making tools and processes, such as Business Case Analysis, Economic Analysis, DSOR Analysis, Decision Tree Analysis, and/or other appropriate best value assessments. At this point, no firm source of support decisions should be made until sufficient data is collected and the risks are determined. (Determination of core capability workload requirements should be made after the system passes Critical Design Review (CDR).) As a result, the analysis results should be used and expanded throughout the program life cycle to:

- Assess alternative contracting approaches based on cost, benefit, and performance outcomes
- Establish a strong foundation for budgetary requirements
- Provide the definitive cost and performance base to be used for contract negotiation
- Provide the cost/performance baseline to be used to measure effectiveness
- Quantify the benefits to be realized

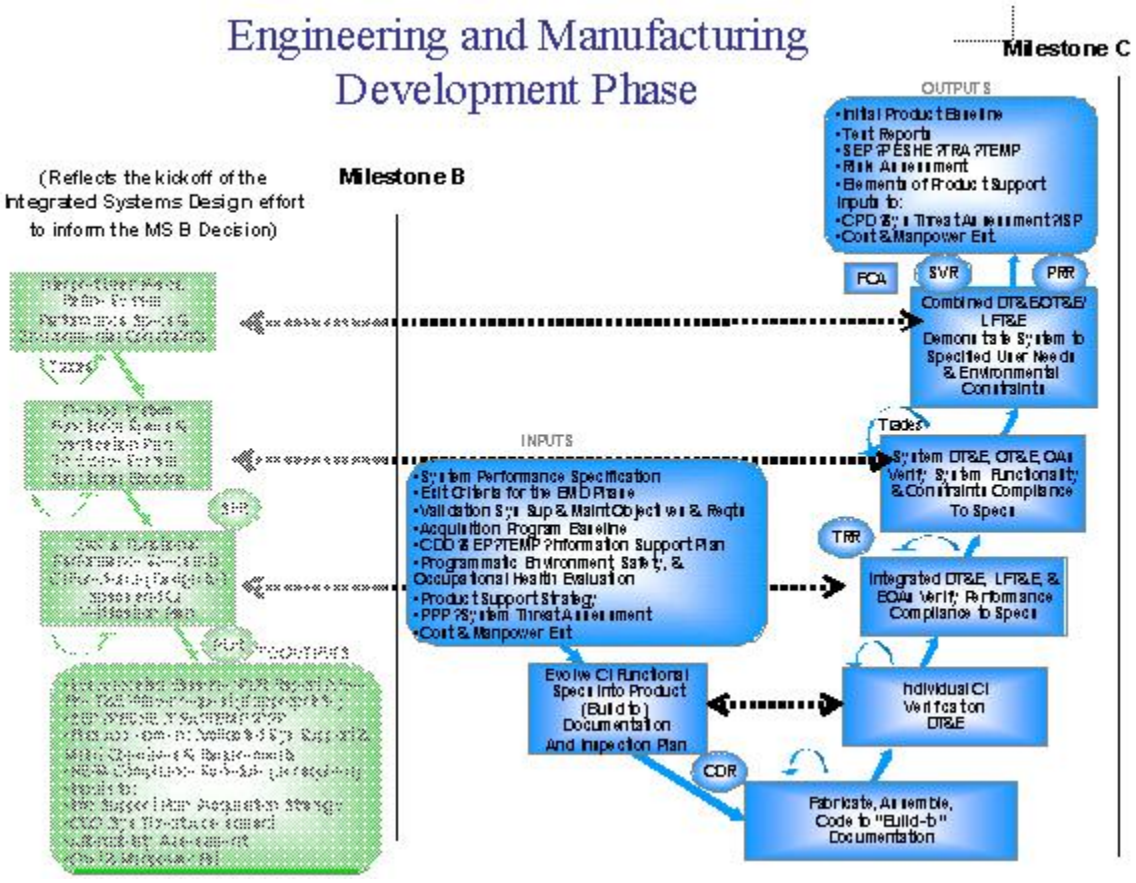


Figure 5.4.3.2.1. System support implications in the Engineering and Manufacturing Development Phase

Almost all of the values used during this phase should be based on engineering estimates and actuals or test results. The level of detail performed by the government team will vary by the extent to which industry is used to achieve the materiel availability in a performance-based logistics contract product support package. (The government's detailed supportability analysis requirements decrease in depth as a direct function of the level the performance standards are set in the contract requirements, the portion of the system covered, and the sustainment functions for which the contractor is responsible.)

Regardless of the contracting approach taken, Supportability Analysis will have to be performed even if only to determine the specific metrics and their respective values that will motivate the right behavior, be aligned with the user requirements and to determine a fair and affordable price. Analysis is also needed to ensure any contracted metrics are aligned with portions of the public infrastructure/supply chain that will support the user. See section 5.4.3.5 for a further description of the best practices that should be used in performing a detailed supportability analysis for any parts of the system in which the government will provide the product support package, vice using a contract with materiel availability as the performance measure.

Reliability Growth. A reliability development/growth effort should be undertaken if the assessed reliability of the system or technology is not above threshold with a safe margin to account for the typical drop experienced when a system transitions from a paper design to fielded conditions. Emphasis should be placed on discovering and mitigating failure modes throughout the system design and development process, since relying solely on testing as a means of improving reliability has been shown to be risky and costly. Consideration should be given to using such practices as physics of failure reviews, environmental stress screening, and highly accelerated life testing. A test analysis and fix program should be implemented to increase reliability and it should be expanded as more of the hardware (including prototypes) is tested and operated by the users. Using this process, failure modes may be found through analysis and testing are then eliminated or reduced by design or process changes as appropriate. Shortchanging this effort early in development, particularly at the subsystem and component level, is a frequent cause of later program delays and cost increases as the flaws inevitably show up in system level performance.

5.4.3.2.1. Life-Cycle Sustainment Plan

The LCSP should be used as a PM management tool to help manage, align the program's efforts and manage the sustainment related risk focusing on the implementation of the product support package. (See figure 5.4.3.2.1.F1 for LCSP focus areas for this phase.) The LCSP further expands on the product support package implementation strategy, maintenance concept (including the depot maintenance requirements and the implications of core requirements), and the technical data required to accomplish maintenance by providing a description of what is expected from each of the stakeholders. In addition to refining and expanding on earlier versions,

it should evolve over the phase and focus on the sustainment implementation planning, program schedule and any special items. Each of the sections should be addressed with specific attention to the following areas:

Sustainment Implementation Plan

- **Supportability Design characteristics** – Describes the key design characteristics included in the contract and how demonstrated performance is tied to incentives. In addition to the design characteristics, it should also include specific information on the subsystems with diagnostics and/or prognostics features and their status.
- **Supportability Analysis Process** – This should describe the processes to establish the requirements for all logistic elements and keep them aligned/balanced as the design and supply chain evolve highlighting how the process has evolved over the phase, with emphasis on the Core Analysis, Source of Repair Analysis (SORA) and DSOR Analysis.
- **Fielding the Product Support Package** – Describes the approach for fielding the product support package, including the major steps in developing and fielding each logistics element describing who is doing what, where, and when with the associated budgets described in the Funding/Budget section. There is no specific format or breakdown required and the level of detail will vary depending on the extent to which outcome based contracts are used, but the following major categories should be addressed:
    - **Maintenance Plan and Requirements** – This should describe the management approach for developing and implementing the maintenance requirements, highlighting how it has changed over the phase.
    - **Technical Data (Paper Based and/or Electronic-Interactive)** – Describes the approach for managing technical data to sustain the program (including for operations, maintenance and re-procurement). This section should summarize the data management strategy by describing the approach for the access, acquisition, sustainment, maintenance, and use of the technical data package over the life cycle, regardless of the contracting strategy or form used. The section should include the data management approach (e.g., use of deferred ordering, priced options for acquiring rights, data escrow) and the government rights (both unlimited and limited) for the data developed at government and private expense. The strategy should be described in sufficient detail to identify and convey a clear understanding of the data approach needed for the entire life cycle. In addition to indicating the extent to which technical data will be distributed to the users in a standards based digital format, the LCSP should indicate how the interactive electronic technical manuals will be sustained and replaced, as well as the process being put into place to ensure the technical data stays in sync with the system configuration, evolving maintenance/ operational procedures, procurement/sustainment strategies, and user issues/input so that changes can be quickly incorporated and distributed to the users.
    - **Support, Test & Calibration Equipment** – Describes the process and management approach for developing and fielding the capabilities to test and

service the system (both embedded and external). The technology being used and how it will be fielded should be described in general terms, but the details by subsystem and what characteristics being measured should be described in supporting documents. The section should also describe the management structure/software capabilities being put into place to improve the built in test, prognostics and diagnostics capabilities as experience/knowledge is gained and technology advances.

- **Manpower & Training/Computer Based Training. -** The approach, locations and schedule for fielding training equipment, material, courses and training should be summarized. (See Chapter 6 for additional information.) The approach for developing each of the elements, with emphasis on key interface points with the other logistics elements (e.g., maintenance plan, test equipment) should also be addressed.
- **Supply Support (Spare/Repair Parts)** – Describes the process and management approach for developing the spares requirements and fielding them to achieve materiel availability. It should also describe the program's supply chain management concept and approach. This should include the extent to which the program is taking advantage of any existing supply chain processes from other systems and the triggers used to indicate potential process changes or PM intervention are needed.
- **Packaging Handling Storage & Transportation** – Describes the approach for these elements with emphasis on how IUID/SIM are being implemented and used. While the details may be articulated in an IUID/SIM Plan, the LCSP should identify the:
  - IUID goals, objectives and how it is being used in information or materiel handling processes
  - Stakeholders involved with the development and implementation of the strategy, including the coordination with other organizations/industry to leverage components, support processes, or information systems
  - Extent to which IUID is being applied (including the current status relative to the budget for IUID parts marking, IUID data management and SIM)
  - Technology being used to mark the parts (e.g., RFID, laser marking) and the extent to which each is being used
- **Facilities** – Describes total facilities' requirements and the plan for providing any unique or new facilities, any facilities modifications, and any interim facilities required to support the program.

- **Sustaining the System** – Describes how systems engineering and life-cycle management strategies will be used to sustain the metrics, including how ranges and triggers will be used for each metric. The focus should be on understanding the cost and logistics infrastructure and footprint associated with meeting the availability requirements and the process to track, control, and/or reduce them over the life cycle.

Program Schedule – Shows how major actions/events for the logistics elements fit with the overall program master schedule. Focus should be on the interfaces and dependences between

the elements. It should update the prior schedule information and include schedule information on the DSOR Analysis.

Special Interest Items – Describes any additional key technologies, initiatives or enablers the program is using to implement the sustainment strategy the program wishes to highlight. For example it should also describe how DMSMS planning is integrated into the acquisition and sustainment approaches, as well as the initiatives in place or planned for public private partnerships.

The level of detail required is dependent on the level required to provide a firm understanding of the approach and the degree to which outcome based contracts and/or agreements are being used. During this phase, the PM should describe the strategy for implementing outcome based contracts, including the level that will be covered by performance-based incentives tied to measured outcome metrics at a predetermined price. It should include the schedule reflecting the plan for reaching the projected end state coverage. If the program is using performance contracts for something other than materiel availability, the LCSP should describe the functions included in the contract (e.g., supply support, reliability improvement, transportation, manpower)

1. Current Program Description - Describes how sustainment considerations are being implemented in the program

1.1 Sustainment and Maintenance Concepts

1.2 Sustainment Acquisition Strategy

1.3 Sustainment Funding/Budget - Detailing Procurement and O&M categories in sufficient detail so stakeholder understand the resources planned to support the program

	Prior	Current Yr	FY+1	FY+2	FY+3	FY+4	FY+5	FY+6	Pgm Completion
RDT&E Rqd									
RDT&E Budget									
Procurement Rqd									
Procurement Budget									
O&M Rqd									
O&M Budget									
Milcon Rqd									
Milcon Budget									

1.4 Stakeholders

2. Program Performance/System Indicators & Requirements - This section should include each metric along with its definition, objective, threshold, its current and projected values.

2.1 Materiel Availability

2.2 Materiel Reliability

2.3 Mean Down Time

2.4 Ownership Cost

2.5 Additional key enabler metrics

Metric	Objective	Threshold	Currently Demonstrated	Projected Value
Materiel Availability				
Materiel Reliability				
Mean Down Time				
Materiel Ownership Cost				
Others				

3. Sustainment Implementation Plan

3.1 Supportability Design Characteristics - Describes the key requirements included in the design specification.

3.2 Supportability Analysis Process - Describes the processes (including Core Assessment/DSOR/ SORA) included in the Systems Engineering Plan being used to establish and keep the product support elements in balance in achieving the Sustainment KPP/KSAs.

3.3 Product Support Package - Describes the major product support elements and plan for fielding the PSP meeting the outcome requirements within statutory and Component mandates.

3.4 Sustaining the Weapon System - Describes the systems engineering and management strategies (including partnerships) to sustain the metrics including how ranges and triggers will be used.

4. Program Schedule - Shows major sustainment actions/events

5. Special Interest Items - Describes any additional information on key technologies, initiatives or enablers the program is using

Figure 5.4.3.2.1.F1. Notional LCSP Focus During Design & Production

5.4.3.2.2. Technical Reviews in Engineering and Manufacturing Development

Regardless of the acquisition strategy chosen relative to PDR timing and prototyping, any remaining initial systems design activities and reviews not finished during the Technology Development phase (i.e., System Requirements Review (SRR), System Functional Review (SFR), or Preliminary Design Review (PDR)) are completed early in the EMD phase. Section 5.4.2.2.3 provides a description of the sustainment aspects that should be considered for each review and is not repeated in this section. If the PDR was not conducted prior to Milestone B, the PM should include the results of the sustainment assessment in the PDR report and Post-PDR Assessment.

5.4.3.2.2.1. Sustainment Considerations in the Critical Design Review (CDR)

The CDR helps to ensure the system can satisfy the CDD requirements within the allocated budget, staffing and schedule. Details can be found in section 4.3.3.4.2, but in summary the CDR results in an initial product baseline for the system, hardware, software, maintainability, supportability, and the product support elements, including support equipment, training systems, and technical data. Subsystem detailed designs and logistics elements are evaluated during the review to determine whether they correctly implement system requirements and if the system is mature enough to proceed into fabrication, demonstration, and test.

Product support IPT members, as well as independent sustainment subject matter experts, should participate to ensure the design includes the supportability requirements and the support strategy contained in the Life-Cycle Sustainment Plan (LCSP) are consistent with the product baseline and the projected sustainment metrics (e.g., reliability, maintainability) and other supportability features. The PM should include the results of the CDR sustainment assessment in the Post-CDR report and Post-PDR Assessment. For the system and key product support elements as appropriate, this involves ensuring the:

- Supportability requirement enablers, such as Human Systems Integration (HSI) design features, inclusive of the environment, safety and occupational health risk reduction features, are included in the design.
- Failure Mode Effects and Criticality Analysis have been completed and any remaining subsystem requirements for the product support package elements design are complete.
- Key sustainment characteristic drivers (including critical manufacturing processes to achieve them) have been identified, and an estimate of system reliability based on demonstrated reliability rates and other sustainment drivers are being used in developing the product support package.

- Development testing results are used to update the sustainment metric projection estimates and any planned corrective actions to hardware/software deficiencies have been identified.
- Test success criteria for any remaining development testing and operational testing plans (for testing both operationally effective and suitable) for key sustainment enablers or drivers requirements are complete. If the test results to date do not indicate the operational test success is likely or risk has increased, new developmental and operational testing criteria and plans should be considered, along with fall-back plans.
- Program sustainment development efforts with corresponding schedules, including system fabrication, test, and software critical path drivers, are included in LCSP updates.
- Updated Cost Analysis Requirements Description (CARD) (or a CARD-like document) based on the initial product baseline, captures the key program sustainment cost drivers, development costs, production costs, operation and support costs for all aspects of sustainment and HSI.

5.4.3.2.2.2. Sustainment Considerations in the Test Readiness Review (TRR)

The TRR helps to ensure the subsystem or system is ready to proceed into a formal test. Details can be found in section 4.3.3.4.3, but in summary it assesses test objectives, test methods and procedures, test scope, and safety confirming test resources have been properly identified and coordinated. Consequently, there are two primary logistics roles in the TRR. One is to help ensure the test is properly planned and resourced (e.g., people, facilities, data systems, support equipment, and any other logistics elements) to achieve the test objectives. The second role is to ensure the tests will identify and help control risk by verifying and validating key sustainment drivers are in place to achieve the Sustainment KPP and KSAs. This can be accomplished by building off the system performance tests as well as structuring specific tests and demonstrations focused on sustainment drivers. Regardless of stage of development or the level of testing (component, subsystem, or system), the basic tenets contained in section 4.3.3.4.3 apply. This includes, but is not limited to, identifying the:

- Test purpose and exit criteria.
- Expected result, test success criteria, and how the test results will affect the program.
- Risks that will be mitigated by the test and which will remain.
- Fall-back plan should a technical issue or showstopper arise during testing.

5.4.3.2.2.3. Sustainment Considerations in the System Verification Review (SVR)

The SVR is a product and process assessment to ensure the system can proceed into production within cost, staffing, schedule, and other system constraints with an acceptable risk level. Details can be found in section 4.3.3.4.5 but in summary the SVR assesses the system functionality, determining if it meets the functional requirements, and verifies final product performance. The

SVR is often conducted concurrently with the Production Readiness Review (section 4.3.3.4.7) and Functional Configuration Audit (section 4.3.3.4.6). Product support IPT members as well as independent sustainment subject matter experts should participate to:

- Address system supportability and, based on developmental testing or analysis whether the sustainment features will satisfy the Capability Development Document/draft Capability Production Document and Sustainment KPP/KSAs.
- Adequate processes are in place so the sustainment performance metrics can be used to help the program to succeed in meeting user needs.
- Ascertain if the system is supportable within the procurement, operations, and support budgets.

5.4.3.2.2.4. Sustainment Considerations in the Functional Configuration Audit (FCA)

FCA is essentially a review of an item's test/analysis data to validate the intended function or performance stated in its specification is met. See section 4.3.3.4.6 for additional details. From a sustainment perspective, the FCA should include auditing the testing and analysis performed to date to ensure the results indicate system compliance with the applicable Sustainment KPPs, KSAs, and derived supportability requirements as reflected in the functional baseline. In addition, to help ensure a system will be sustainable, key elements of the product support system should also undergo a FCA.

5.4.3.2.2.5. Sustainment Considerations in the Production Readiness Review (PRR)

The PRR determines whether the design is ready for production and if the producer has accomplished adequate production and product support planning. Details can be found in section 4.3.3.4.7, but in summary it determines if production or production preparations incur unacceptable risks that might breach schedule, performance, cost, or other established criteria thresholds. The review evaluates the full, production configured system to determine if it correctly implements all system requirements, including embedded sustainment enablers. Product support IPT members, as well as independent sustainment subject matter experts, should participate to ascertain that the product support baseline has been established, documented and the:

- Supportability design features are mature enough to be incorporated into the design within the budget, schedule or other design constraints (e.g., weight, size, bandwidth).
- Product support is properly planned and implementation will meet sustainment objectives and requirements.
- System is supportable within the procurement, operations, and support budgets and fielded infrastructure.
- Initial product support package and supply chain are ready to support production output.

- Processes in place are adequate for sustainment performance metrics to help the program succeed in meeting user needs.

5.4.3.2.2.6 Technology Readiness Assessment (TRA)

A second TRA is normally conducted prior to Milestone C and may be held concurrently with other technical reviews, specifically the System Verification Review, or Production Readiness Review, to assess the technology maturity. From a sustainment perspective, the TRA should be used to assess the risk and the adequacy of the sustainment drivers to meet the system requirements. (See section 4.3.3.4.8 and 5.4.2.2.3.4 for additional information.)

5.4.3.3. Engineering & Manufacturing Development Phase Results/Exit Criteria

The focus of this phase is to ensure the system design incorporates the critical supportability/ logistics requirements, develops the logistic element capabilities, and demonstrates the key support and sustainment capabilities are mature. Implementing the process contained in figure 5.4.3.2.F1 produces the detailed supportability/logistics requirements and the initial designs. The conclusion of this phase results in the contractual documents required to continue into the Production and Deployment Phase as well as the system prototype logistics equipment and processes. The program should be able to demonstrate acceptable performance in the development, test & evaluation, and operational assessments, to include:

- Demonstrated reliability, availability, maintainability, and sustainment features
- Established and verified product support baselines
- Mature software design
- Acceptable interoperability

Table 5.4.3.3.T1 identifies the most critical documents that should incorporate or address supportability/ logistics considerations. The logistics related data in program deliverables should be updated prior to milestone decisions and to support the various major design reviews (e.g., CDR, and FCA). The key sustainment elements required for low rate initial production systems and initial operational test and evaluation (IOT&E) should be addressed in the LCSP which is summarized in the Acquisition Strategy. Materiel availability enabler driver initiatives should be included in the RFP as well as the Source Selection Plan.

From a logistics perspective, the exit documents should focus on the results of the maintenance planning process, the materiel availability driver initiatives, and their associated metrics. In addition to updating the support strategy, sustainment funding requirements, key logistics parameter and logistics testing criteria, the annual determination of the distribution of maintenance workloads required by statute, an auditable depot level maintenance core capability and workload assessment should be completed bi-annually.

Entry Documents:
Initial Capabilities Document and Capability Development Document
Acquisition Strategy
Acquisition Program Baseline
Preliminary Design Review Results
Developmental Test and Evaluation Report
Operational Test Plan and Test & Evaluation Master Plan (TEMP)
Life-Cycle Sustainment Plan
Exit Documents:
Update documents from MS B
Capability Production Document
Approved Maintenance Plans
Life-Cycle Sustainment Plan

Table 5.4.3.3.T1. Sustainment Considerations in EMD

5.4.3.4. Sustainment Considerations in the Engineering and Manufacturing Development Phase

5.4.3.4.1. Sustainment Metrics

During this phase, the focus should be on achieving the objective range value estimate for each of the Sustainment KPP/KSAs, along with their supporting driver metrics, and on further analysis (including analysis of the results of any demonstrations that have been performed). The analysis should be performed to:

- Ensure the various metric performance values are consistent with each other as each is refined
- Ensure the design/production process does not degrade the system's ability to meet the sustainment metrics
- Identify the operation impacts the sustainment metrics enablers will have on mission success and materiel availability

The models for establishing and tracking projecting expected values should be refined and the requirements for the metrics should be further allocated to the equipment level. Key metrics data should be collecting and used to validate the models, evaluate technical performance, evaluate system maturity and determine the logistics footprint. The key enabling requirements to achieve the sustainment metrics should be included in the system specification and PBAs. Detailed test criteria should be developed for each metric (including any key dependent enabling

technologies) to provide information about risk and risk mitigation as the development and testing continue. The sustainment test strategy/requirements should be documented in the TEMP.

5.4.3.4.2. Technology Refreshment and Obsolescence Management

The extensive life of our systems and rapid technology change has heightened the importance of technology refreshment and obsolescence management. Consequently, successful parts management necessitates the need to address diminishing manufacturing sources and material shortages in the proposal, design, and sustainment phases of a product (to include the systems and support elements). The PM should develop a proactive approach to effectively resolve obsolescence problems before they have an adverse impact on the LCC and system availability. The following are potential approaches the PM should consider:

- Design features that facilitate change/insertion of new technology
- Establishing a rigorous change management process for life-cycle support.
- Using performance-based logistics contracts that provide significant latitude to manage technology refreshment. This includes ensuring they are incentivized to maintain currency with state-of-the-art technology and use readily available items to avoid the high cost of diminishing manufacturing sources and materiel shortages over the system's life.

5.4.3.4.3. Sources of Support

DoD Components should operate an integrated, synchronized, total system supply chain to meet user requirements for information and materiel. Competition throughout the life cycle, including during sustainment, is integral to providing best value logistics processes. Consequently, per Public Law 111-23, major weapon systems shall, to the maximum extent practicable and consistent with statutory requirements, ensure maintenance and sustainment contracts are competitively awarded and given full consideration to all sources (including sources that partner or subcontract with public or private sector repair activities).

The Sustainment KPP/KSAs allow the acquisition and sustainment communities to focus their efforts from the user's perspective, rather than focusing on any segment of the chain in isolation. This consistent focus on a common outcome (affordable materiel availability) across the supply chain reduces the potential for disconnects during the multiple hand offs across the various links in the supply chain. Consequently, in satisfying the user's needs under the total life-cycle system management approach, the PM is responsible for:

- Determining the appropriate set of metrics to align the various supply chain segments to achieve materiel availability. The specific metrics and their values should be determined regardless of who is executing the action to meet the user needs in the operational environment and be based on the system characteristics.
- Selecting the sources of support to sustain the system. Working with the maintenance community, the PM should use the most effective sources of support that optimize the

balance of performance and life-cycle cost, consistent with statutory requirements and required military capability. The sources may be organic or commercial, but the focus should be on optimizing customer support and achieving maximum system availability at the lowest LCC. In making the determination, the PM shall (DoD Instruction 5000.02, Enclosure 8, paragraph 2.d.) work with the manpower community to determine the most efficient and cost effective mix of DoD manpower and contract support.

- Providing the mechanisms and logistics elements (including technical data) to implement the source of support decisions. In doing so, the strategy and resources required to implement the strategy should foster and ensure competition throughout the life of the system.
- Monitoring execution against the metrics to ensure the respective stakeholders are engaged in providing the system support to the user. Effective supply chain management requires data collection and data sharing within and between all elements of the supply chain (public and private). There should be a process to collect data throughout the manufacturing process and operations period so the data may be mined for product and process improvements using trend analysis to effectively communicate/collaborate with a shared understanding of the environment.

User and Provider Collaboration. Implementation of the life-cycle management approach places a premium on collaboration to promote user confidence in the logistics process in building a responsive, cost-effective capacity to ensure users get the materiel they need, when they need it, with complete status information. Supply chain management in particular requires PMs to collaborate with users (e.g., the force providers, the Combatant Commands, and the DoD Components of those commands) to determine optimal logistics strategies tailored to meet the users' needs and expectations and should produce a performance-based agreement codifying the negotiated user requirements and performance expectations (DoD Directive 5000.01). The PM should ensure user support is based on collaborative planning, resulting in realistic performance expectations established through performance-based agreements. These agreements should be negotiated in conjunction with the product support integrator, support providers, and the service providers (e.g., maintenance, supply, distribution centers, transportation providers).

Program managers can contract for performance-based sustainment as part of or as the total sustainment strategy. Contracts can be very powerful tools when support is focused on the customer and entire supply chain thereby mitigating or eliminating conflicting commodity priorities. Any sustainment contracts used should be focused to exploit supply chain processes and systems as well as to provide flexible and timely materiel support response during crises and joint operations. Regardless of the strategy taken, the PM must provide for long-term access to the data required for competitive sourcing of systems support and maintenance throughout its life cycle (see DoD Directive 4151.18 for additional information and guidance). The following major elements of the supply chain should be considered.

5.4.3.4.3.1. Maintenance

Program managers should determine the most effective levels of maintenance and sources based on materiel availability and cost factors. In early deployments the best value may be to use existing contractor capabilities for interim support. However core sustaining workload must be accomplished in Government owned facilities with Government owned equipment and personnel. If it has not already been completed, the PM should perform the analysis discussed in sections 5.2.1.2 and 5.4.2.2.2 to determine the maintenance source that complies with statutory requirements, operational readiness and best value for non core workloads.

Government and Industry Support Partnerships. In meeting the sustainment requirements, maintenance public private partnerships are the preferred arrangements for maintaining and repairing DoD weapon systems, hardware, equipment, and software. Public Private Partnerships can contribute to more effective DoD sustainment operations, can introduce innovative processes or technology, and enable the economical sustainment of organic capabilities. Delineating specific performance objectives in the mutual interests of both sectors, providing financial incentives for attaining the objectives, ensuring responsibilities are clearly assigned across the widest possible segment of maintenance workload requirements can result in:

- Improving DoD depot maintenance operations by combining the best of commercial processes and practices within the Department's own extensive maintenance capabilities
- Industry leveraging the depot's skilled artisans along with best commercial best practices.
- Increasing availability at reduced total ownership costs and increased reliability for new and legacy systems

Figure 5.4.3.4.3.1.F1 depicts some of the key benefits of well designed public private partnerships. However, care is needed when third party are involved. For example for information technology/software support some level of organic support needs to be resident and none of the support can be sent to non approved third party countries (i.e. India, China etc) without thorough analysis and State Department approval. Further examples and discussion of public private partnerships can be found in DoDI 4151.21 and on the Acquisition Community Connection web site.

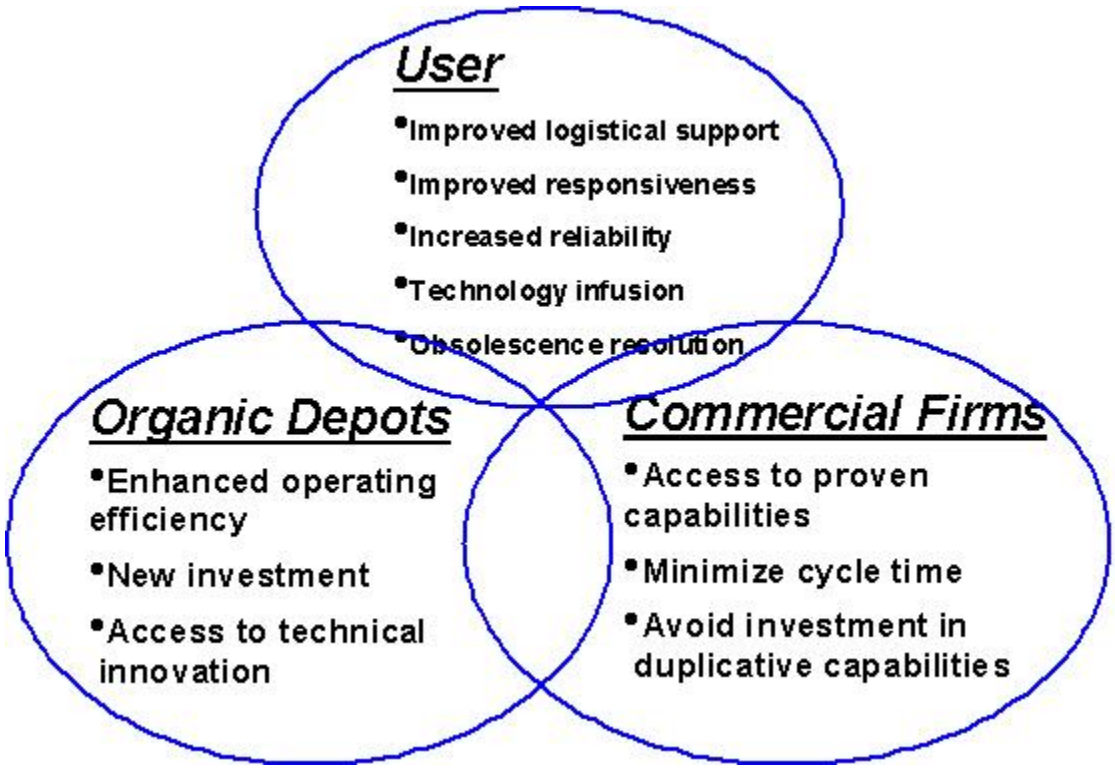


Figure 5.4.3.4.3.1.F1. Public Private Partnership Opportunities

5.4.3.4.3.2. Supply

Supply requirements are determined as a part of the maintenance planning process. However, DoD policy gives the program manager latitude in selecting a source of supply support, including support management functions, that maximizes service to the user while minimizing cost. A framework for developing, improving, and conducting supply chain management activities to satisfy support element requirements is a vital link in systems sustainment because skilled labor and advanced technology repair equipment mean little without the right part in the right place at the right time. Consequently, the PM should select a source of supply support that gives sufficient control over financial and support functions to effectively make trade-off decisions that affect materiel availability and cost.

Competitive Process. Supply support may be included as part of the overall system procurement or as a separate competition. The competitive selection process should result in a contract with a commercial source and/or an agreement with an organic source that prescribes a level of performance in terms of materiel availability and cost. The PM may use a competitive process to select the best value supply support provider or include supply support in an overarching performance-based logistics support arrangement. While access to multiple sources of supply may be encouraged to reduce the risks associated with a single source, it is imperative that a single entity be established as a focal point of responsibility. Particular attention should be given

to prime vendor contracts for specific commodities and virtual prime vendor contracts for a wide range of parts support for specific subsystems. Additional guidance appears in DoD Directive 4140.1 and DoD 4140.1-R.

Organic Supply Source of Support. The PM should select organic supply sources of support when they offer the best value. (DoD Directive 5000.01, E1.1.17) When changing the support strategy for fielded equipment from organic to contractor support or from contractor to organic support, DoD owned inventory that is unique to that system should be addressed in the source of support decision.

5.4.3.4.3.3. Transportation

The PM is encouraged to determine the best overall support strategy for the customer to include the use of all available transportation alternatives, including those provided by original equipment manufacturers (OEMs), third party logistics providers, or commercial transportation providers. These alternatives may include the use of commercial transportation services and facilities to the maximum extent practicable; the use of organic transportation consistent with military needs; or the combination of both commercial and organic transportation to support customer requirements. As in supply support, the PM should strive to structure a support arrangement, such as performance-based logistics contracts, that will consolidate the responsibility for transportation in a single entity. Regardless of the approach taken, when making the transportation source decision the PM needs to ensure the entire end-to-end chain is considered including the "last mile" aspects along with any required implementing technology (e.g., IUID).

In considering transportation options, the PM should also plan for transition of the supply and distribution chain from normal operations to expeditionary operations in austere locations that are not served, at least initially, by commercial transportation services and facilities. Transportation alternatives in contractual arrangements must require the contractor to comply with established business rules, when the DoD organic distribution system is used in lieu of or with the commercial transportation service. All contractual arrangements requiring that deliveries be made using door-to-door commercial transportation must include a provision that requires vendors to notify the contracting officer or the contracting officer's designee when they are unable to use door-to-door commercial transportation and to request alternate shipping instructions. The contracting officer or contracting officer's designee must expeditiously provide alternate shipping instructions and make the appropriate contract price adjustments. For additional information, see the on-line Defense Transportation Policy Library.

Arms, Ammunition, and Explosives. PMs should refer to DoD 4500.9-R, Defense Transportation Regulation, Part 2, and DoD Manual 5100.76-M, Physical Security of Sensitive Conventional Arms, Ammunition and Explosives (AA&E), for transportation and security criteria regarding the movement of arms, ammunition, and explosives. Contract provisions should apply to the prime contractor and all subcontractors.

5.4.3.4.4. Other Considerations

Design Impact. Design alternatives should continue to be considered to help mitigate sustainment risks and reduce LCC and logistics footprint as the design is refined.

Support Strategy. In refining and determining the detailed supportability requirements developed in the earlier phases, the PM should take into consideration the various alternatives that can be cost effectively implemented to achieve the Sustainment KPP and KSAs and to reduce program risks. The following are also aspects that should continue to be considered during this phase in designing and implementing the support strategy:

- **Interservice servicing agreements** to take advantage of joint capabilities by drawing support from other DoD Components and Allies. In developing the support strategy, the long term potential of Acquisition and Cross Servicing Agreements (ACSAs) to help reduce the logistics infrastructure and footprint should be considered. For further discussion including information on the legal authority for the acquisition and reciprocal transfer of logistic support, supplies, and services from eligible countries and international organizations, see section 11.2.3 and DoDD 2010.9.)
- **Adopting DoD Enterprise initiatives** to reduce ownership costs. For example adopting DoD's enterprise architecture for the information infrastructure, processes, data, data standards, business rules, operating requirements, and information exchanges can facilitate interoperability and ownership costs.

5.4.3.5. Best Practices during the System Engineering and Manufacturing Development Phase

Modeling and simulation combined with supportability analysis are important best practices to design and develop the individual logistic elements required to implement the support strategy. During this phase they are applied to lower and lower levels of detail as the design matures. The supportability analysis should continue to be used to determine the relative cost vs. benefits of different support strategies (including the source of support decisions). The data should be refined and the results included in the LCSP and used to support contract negotiations.

Once logistics elements are developed and prototyped, modeling and simulation can also be used to provide confidence the sustainment metrics will mature to sufficient levels when the system and supply chain are deployed. This is accomplished with the use of models that take test results and predict likely capabilities. The same concepts are applied to provide confidence levels of what the enabling technologies will be able to achieve in the operational environment and identify any anticipated constraints. All of these factors are then used to project the mature sustainment metric values and their associated confidence levels for the projected Concept of Operations.

5.4.4. Sustainment in the Production and Deployment Phase

5.4.4.1. Overview

The logistics purpose in this phase is to achieve a materiel availability capability that satisfies mission needs. Milestone C authorizes entry into Low Rate Initial Production, at which time the design should be mature. The supportability design feature requirements should have been verified and validated as operationally suitable and effective at an affordable cost. At this point, the support requirements should be fully defined and performance-based product support agreements and funding expectations documented and signed. Funding should also be identified

and available for testing and implementation of the performance-based strategy. Once operational test and evaluations have determined the effectiveness, suitability, and supportability of the system, the full rate production and deployment decision is made.

5.4.4.2. Activities/Processes

During this phase, the emphasis is on finalizing equipment product support packages/ maintenance plans, managing and deploying the initial sustainment capabilities, and demonstrating the product support capabilities and effectiveness. Once they have been demonstrated, the emphasis is on fully fielding and implementing the sustainment capabilities to provide the users the capabilities identified in their requirements documents. Measuring the product sustainment package's effectiveness (including the associated supply chain) is an important aspect of the management responsibilities in this phase. Figure 5.4.4.2.F1 highlights the key phase activities.

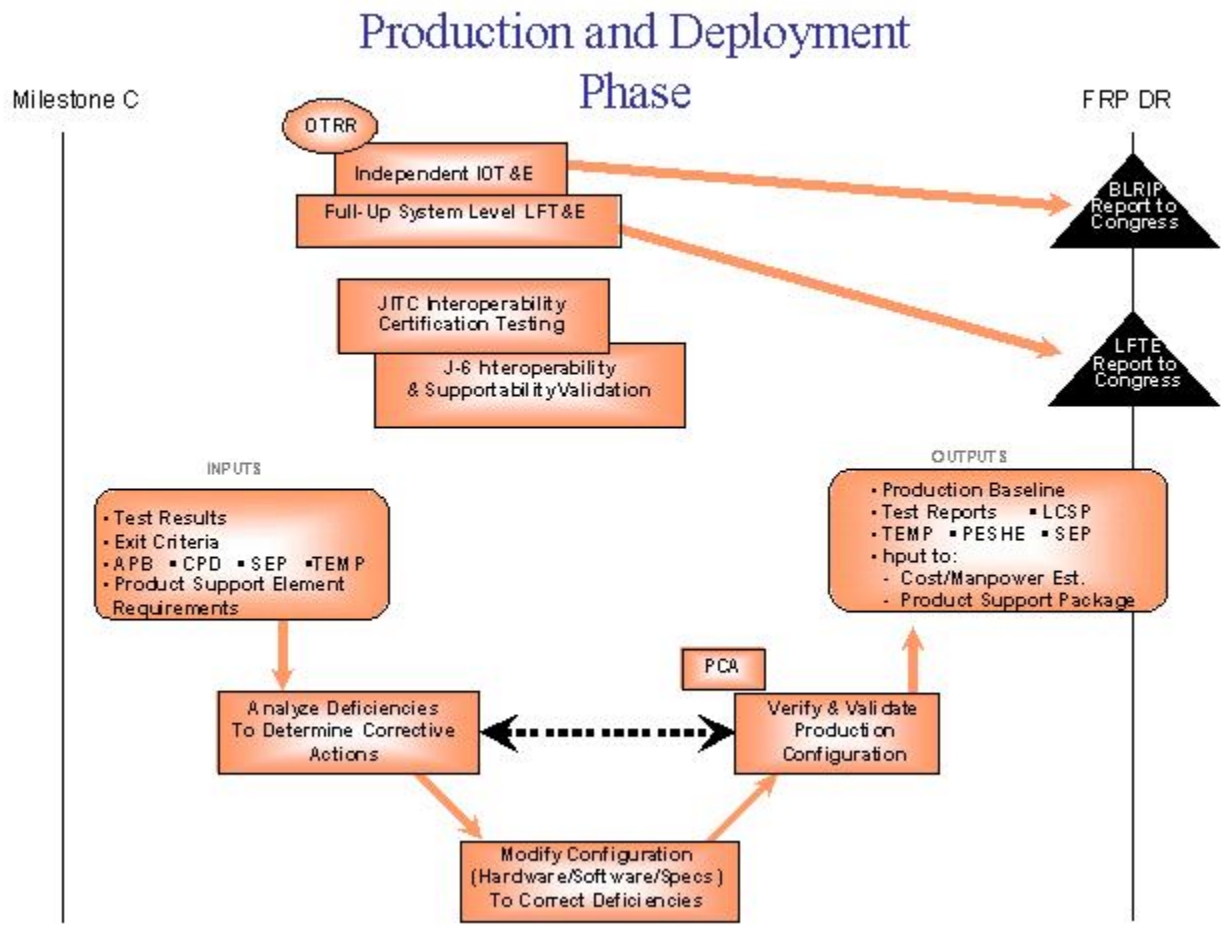


Figure 5.4.4.2.F1. System support implications in the Production and Deployment Phase

5.4.4.2.1. Managing Product Support Package Fielding

The following are key program manager responsibilities in this phase:

- Ensuring actions are taken to provide the user support required to sustain the system within the budget provided, including highlighting to senior management the consequences and impacts on the Sustainment KPP/KSAs of budget constraints.
- Coordinating with the contractors, supply chain and operators to ensure each understands and is implementing responsibilities in accordance with the LCSP in an integrated fashion.
- Monitoring any changes to the design, operational environment and supply chain and adjusting the logistics elements within the product support package accordingly.
- Looking for improvements to reduce the product support package cost.

During this phase, the reliability of contractor cost and performance data should be verified by monitoring contracts. Increased use of Defense Contract Management Agency and Defense Contract Audit Agency in overseeing contracts should be considered.

5.4.4.2.2. Maintenance Supportability Considerations

10 USC 2464 requires the establishment of the capabilities necessary to maintain and repair systems and other military equipment required to support military contingencies (i.e., core capabilities) at Government-owned, Government-operated facilities not later than four years after achieving initial operating capability. During the production and deployment phase, it is imperative for the PMs and Program Executive Officers to ensure the prior planning for maintenance support is executed to meet the supportability requirements of the system and/or subsystems. If organic depot maintenance is a portion of the selected supportability strategy, it will require the activation of the requisite organic depot maintenance capabilities.

5.4.4.2.3. Life-Cycle Sustainment Plan

The LCSP should be used to help manage the program's fielding efforts. (See figure 5.4.4.2.3.F1 for notional LCSP focus areas for this phase.) In addition to refining and expanding on earlier versions, it should focus on the product support implementation plan and program schedule, with emphasis on putting into place the continuous process improvement (CPI) management structure to review processes and remove bottlenecks or constraints encountered by the user. The following are aspects that should be emphasized along with the projected sustainment metric values by fiscal year over the FYDP:

Stakeholders – In this phase, the LCSP should further expand on the stakeholder roles in executing the sustainment strategy by describing the relationships and responsibilities with key players, especially relative to any long term PBAs. For each PBA (including those planned or being put into place), the LCSP should address the performance outcome metrics, agreement

length, resources tied to the agreement (including color of money) and who has agreed to/signed it.

Sustaining the Weapon System – Describes how systems engineering and life-cycle management strategies are being used to sustain the metrics, including how ranges and triggers are used for each. The focus should be on understanding the cost and logistics infrastructure and footprint associated with meeting the availability requirements and on the process to track, control and/or reduce them over the life cycle. The following are potential areas to be included:

- The feedback mechanisms being put to place to collect RCM and other logistics performance data to improve design and maintenance (e.g., reliability data, actual corrosion data) so that additional proactive prevention/correction steps can be taken and/or the logistics elements can be adjusted.
- The health and usage management system including the management structure/software capabilities being put into place to improve the prognostics & diagnostics capabilities as experience/knowledge is gained and technology advances.

1. Current Program Description - Describes how sustainment considerations are being implemented in the program

1.1 Sustainment and Maintenance Concepts

1.2 Sustainment Acquisition Strategy

1.3 Sustainment Funding/Budget - Detailing Procurement and O&M categories in sufficient detail so stakeholder understand the resources planned to support the program

	Prior	Current Yr	FY+1	FY+2	FY+3	FY+4	FY+5	FY+6	Pgm Completion
RDT&E Rqd									
RDT&E Budget									
Procurement Rqd									
Procurement Budget									
O&M Rqd									
O&M Budget									
Milcon Rqd									
Milcon Budget									

1.4 Stakeholders

2. Program Performance/System Indicators -Includes the actual measured value and its projected value based on current funding/budgets

2.1 Materiel Availability

2.2 Materiel Reliability

2.3 Mean Down Time

2.4 Ownership Cost

2.5 Additional key enabler metrics

Metric	Objective	Threshold	Projected Values						
			Current	FY+1	FY+2	FY+3	FY+4	FY+5	FY+6
Materiel Availability									
Materiel Reliability									
Mean Down Time									
Matl Ownership Cost									
Others									

3. Sustainment Implementation Plan

3.1 Supportability Design Characteristics - Describes key ECP's being implemented.

3.2 Supportability Analysis Requirements - Describes the processes being used to keep the product support elements in balance.

3.3 Product Support Package - Describes key PSP adjustments to reduce risk, sustain or improve the sustainment metrics.

3.4 Sustaining the Weapon System - Describes the systems engineering and management strategies to sustain the metrics including how ranges and triggers are used.

4. Program Schedule - Shows major sustainment actions/events

5. Special Interest Items - Describes additional information on key technologies, initiatives or enablers the program is using

Figure 5.4.4.2.3.F1. Notional Life-Cycle Sustainment Plan Focus During Operations

5.4.4.2.4. Measuring Sustainment Effectiveness

Under the total life-cycle systems management concept, the PM is responsible for the timely fielding of an effective product support package, measuring its effectiveness, and taking corrective actions when shortfalls are uncovered. The most effective time to catch problems is before the system is deployed, so including reliability, maintainability and supportability test requirements in the TEMP should be as important as other performance measures. Sustainment KPP/KSA driver metrics should be monitored thought out the test and deployment process to help provide confidence the system will achieve the sustainment objectives in an operational environment.

5.4.4.2.5. Pre-Initial Operational Capability Supportability Review

This review and its associated analysis should be performed at the DoD Component level in conjunction with the OTRR to:

- Confirm design maturity and configuration of the system
- Determine status of correction of any deficiencies identified
- Confirm configuration control
- Certify product support integrator/providers plan to meet user requirements
- Verify product support integrator/provider agreements/contracts and funding are in place

5.4.4.2.6. Technical Reviews in Production and Deployment

Many of the actions and subsequent results in this phase are reviewed during technical reviews and should be accomplished even if the specific referenced reviews do not occur. The actions and results are tied to the reviews to reflect the relative timeframe in which they should be accomplished.

5.4.4.2.6.1. Sustainment Considerations in the Operational Test Readiness Review (OTRR)

The OTRR is a product and process assessment to ensure the system can proceed into Initial Operational Test and Evaluation with a high probability of successfully completing operational testing. (See section 4.3.4.4.2 for additional information.) Many of the same actions used to prepare for the Test Readiness Review (TRR) should be used in preparation for this review. This test is critical because it provides the users the first real hands-on indication as to whether the system is operationally effective and suitable. Consequently, it is important the product support IPT members as well as independent sustainment subject matter experts participate in the review to ensure the test:

- Is properly planned and resourced (e.g., people, facilities, data systems, support equipment, and any other logistics elements) to achieve the test objectives. The Pre-Initial Operational Capability Supportability Review should be used to support this process.
- Will verify and validate the key sustainment drivers to achieve the Sustainment KPP and KSAs are included. This should include ensuring system reliability, maintainability, and support performance features are included and demonstrated.
- Is structured to include as much of the product support package that will be used in the operational environment. Where this is not possible, prototypes should be used to gain early user feedback on the product support package.

5.4.4.2.6.2. Sustainment Considerations in the Physical Configuration Audit (PCA)

The PCA examines the end-item actual configuration as defined by the Technical Data Package and sets the final production baseline under government control. Details can be found in section 4.3.4.4.3, but in summary the audit verifies that design documentation matches the item specified in the contract. In addition to the standard practice of assuring product verification, the PCA confirms that manufacturing processes, quality control system, measurement and test equipment, product support, and training are adequately planned, tracked, and controlled. As such, this review should be used to ensure the "as-produced" system is compliant with sustainment requirements and objectives. To the extent lead times will allow, ordering the product support package elements should be delayed until this review to ensure they are being bought for the right configuration.

5.4.4.3. Production and Deployment Phase Results/Exit Criteria

The focus of this phase is to deploy the initial sustainment capabilities and once the system (both the system and its product support package) are demonstrated to be operationally suitable and effective to then fully deploy the system. This should be demonstrated by:

- The satisfactory achievement of the sustainment criteria in the Initial Operational Test and Evaluation (IOT&E) and other tests.
- Performance-based product support agreements being in place.
- A fully funded sustainment program in the budget.

Implementing the process depicted in figure 5.4.4.2.F1 provides the materiel required to gain full rate production/deployment approval and produce the product support elements to sustain the system. The conclusion of this phase results in a fully fielded and supported system. Table 5.4.4.3.T1 identifies the most critical documents that should address sustainment considerations. Key logistics information complied during this phase should be used to update the acquisition documents, along with the latest sustainment strategy based on the actual technology development progress and/or follow-on increments if an incremental acquisition strategy is used. Also, the sustainment related data and performance-based requirements should continue to be

included in product and sustainment contracts and agreements to ensure the system is effectively supported.

Entry Documents:
Test and Evaluation Reports
Acquisition Program Baseline
Operational Test Plan and Test & Evaluation Master Plan (TEMP)
Life-Cycle Sustainment Plan
Exit Documents:
Update documents from MS C as appropriate.
Physical Configuration Audit Report
Life-Cycle Sustainment Plan
Information Supportability Certification

Table 5.4.4.3.T1 Sustainment Considerations in Production and Deployment

5.4.4.4. Sustainment Considerations in the Production & Deployment Phase

All the logistics elements should be considered and focus should be on refining and fielding them based on their demonstrated success and on confidence that the requirements will be achieved.

5.4.4.4.1. Sustainment Metrics

The results and experience demonstrated in all the tests (including follow-on operational test & evaluation (FOT&E)) and early operations should be considered in refining the metric estimates. This, along with key supply chain performance and effectiveness measures for similar fielded systems, should be used to increase the confidence levels for the PM's estimates. Supply chain performance, Sustainment KPP/KSAs, and key driver metrics should also be considered in the analysis. Special emphasis should be placed on tracking the metrics for the drivers of key enabler technologies that have been developed for the system or are critical for achieving the required materiel availability. Consideration should be given to revising the product support package and its agreements if major performance shortfalls are found.

5.4.4.4.2. Configuration Management

Special attention should be placed on configuration and data management, as design changes are made to ensure the product support package is developed and fielded to the same

configuration(s) the user will be operating and supporting. Ensuring logistics and sustainment implications are considered and addressed during the Physical Configuration Audit (PCA), Physical Configuration Review, and Operational Test Readiness Review (OTRR) can increase the probability both the system and its support package are deployed in a coordinated fashion.

When multiple production baselines are deployed or if the full product support package is not deployed to support test or operations, the program manager should consider the most effective support method. The alternatives considered can include employing mixes of contractor and organic support over varied performance periods for each configuration. This may result in the consideration of multiple performance agreements and/or support strategies. In determining the best mix, the results from the Production Readiness Review (PRR) and System Verification Review (SVR) should be considered to ensure the logistics elements are developed for all configuration / block increments.

5.4.4.4.3. Contractor Logistics Support/Contractors on the Battlefield (CLS/COTB) Integration, In-Theater

Contractors can provide logistics support over a wide range of options, from interim contractor support covering the initial fielding while the product support package is being deployed, to supporting specific limited operations, to full contractor support. When support strategies employ contractors in a battlefield environment, PMs should, in accordance with Joint Publication 4-0 Chapter 5 and DoD Component implementing guidance, coordinate with affected Combatant Commanders. This coordination must be carried out through the lead DoD Component and ensure functions performed by contractors, together with functions performed by military personnel, and government civilians, are integrated in operations plans (OPLANs) and orders (OPORDs). During this process the Combatant Commanders will:

- Identify operational specific contractor policies and requirements, to include restrictions imposed by international agreements;
- Include contractor related deployment, management, force protection, medical, and other support requirements, in the OPORD or a separate annex; and
- Provide this information to the DoD Components to incorporate into applicable contracts.

The intent of the coordinated planning is to ensure the continuation of essential services in the event the contractor provider is unable (or unwilling) to provide services during a contingency operation. Contingency plans are required for those tasks that have been identified as essential contractor services to provide reasonable assurance of continuation during crisis conditions in accordance with DoD Instruction 3020.37. PMs should also coordinate with the DoD Component manpower authority in advance of contracting for support services to ensure tasks and duties that are designated as inherently governmental or exempt are not contracted.

5.4.4.5. Best Practices during the Production and Deployment Phase

5.4.4.5.1. Supportability Analysis

Supportability Analysis should continue to be expanded in depth and adjusted as necessary based on test results and operational experience. In examining additional information, a conscious decision has to be made as to whether or not the new data warrants a re-examination of previous analyses. Even if the change is not sufficient enough to warrant an adjustment to the support package, an analysis should be performed to assess the risk associated with the new information so key stakeholders can take risk mitigation steps.

Configuration control over the analysis and resulting data becomes important as the design changes. The program should take steps to ensure that as the system changes, the product support package is adjusted to take into account the various configurations the user will encounter and the logistic elements stay in sync.

Even well into operations, programs should evaluate opportunities for transitioning, in whole or part, to performance-based logistics contracts by examining opportunities to leverage public private partnerships. Experience has shown that, even with existing capitalized infrastructure in place, legacy programs can transition to outcome based contracts across the spectrum of subsystem or functional process support segments.

5.4.4.5.2. Modeling and Simulation

M&S continues to support the program improvement efforts by analyzing the impact of proposed design refinement, maintenance processes, and budget alternatives on the sustainment metrics/mission effectiveness. M&S should be used in assessing the alternatives of both the system and its support system (especially the enabling technologies), ensuring all critical metrics are considered in parallel and not at the expense of others. In addition, taking early operational results and predicting likely trends (with confidence levels) can be used to proactively anticipate problems so corrective actions can be taken as the system is fielded to minimize adverse impacts on the users. This also helps to provide confidence the critical sustainment metrics will mature to sufficient levels when the system and supply chain are fully deployed and to identify any anticipated constraints or limitations.

5.4.5. Sustainment in the Operations and Support Phase

5.4.5.1. Overview

In the total life-cycle systems management concept, providing user support and managing the demilitarization/disposal of old systems are the PM's responsibilities. During this phase, the PM is the system focal point to the user and should continually assess the sustainability effectiveness of the fielded systems, adjusting the program as required to support the user.

Users require readiness and operational effectiveness (i.e., systems accomplishing their missions) in accordance with their design parameters in an operational environment. Systems, regardless of the application of design for supportability, suffer varying stresses during actual deployment and use. Consequently, the PM should apply the systems engineering processes used in acquisition throughout the entire life cycle. The difference is that during this phase actual use data including user feedback, failure reports, and discrepancy reports rather then engineering estimates are used.

While acquisition phase activities are important to designing and implementing a successful and affordable sustainment strategy, the ultimate measure of success is supporting the user after the system has been deployed for use. Accordingly, the PM and DoD Components should conduct periodic assessments of system support outcomes comparing actual vs. expected levels of performance and support. The assessments require close coordination with the user, support providers and appropriate systems engineering IPTs. They should be structured to:

- Monitor system usage and supply chain against design baseline criteria and assumptions.
- Review and triage all use data and supplier data to determine operational hazards/safety risks, as well as readiness degraders.
- Develop alternatives to resolve critical safety and readiness degrading issues.
- Identify sub-optimal performers in the fielded product support system, and correct them through rebalanced logistics elements or changes to the maintenance program.

- Enhance the performance and cost-effectiveness of the end-to-end supply chain to ensure materiel readiness continues to meet user needs.
- Identify redesign opportunities to enhance system effectiveness.

5.4.5.2. Activities/Processes

During this phase, the focus is on supporting the user by executing the sustainment program and on making adjustments based on effectiveness and operating conditions using systems engineering principles. However, the PM should not undertake depot maintenance source of support decisions without consultation with accountable military department logistics officials to ensure the DoD Component depot maintenance 50 percent limitation statutory requirement is being met. Figure 5.4.5.2.F1 highlights the key sustainability and product support activities.

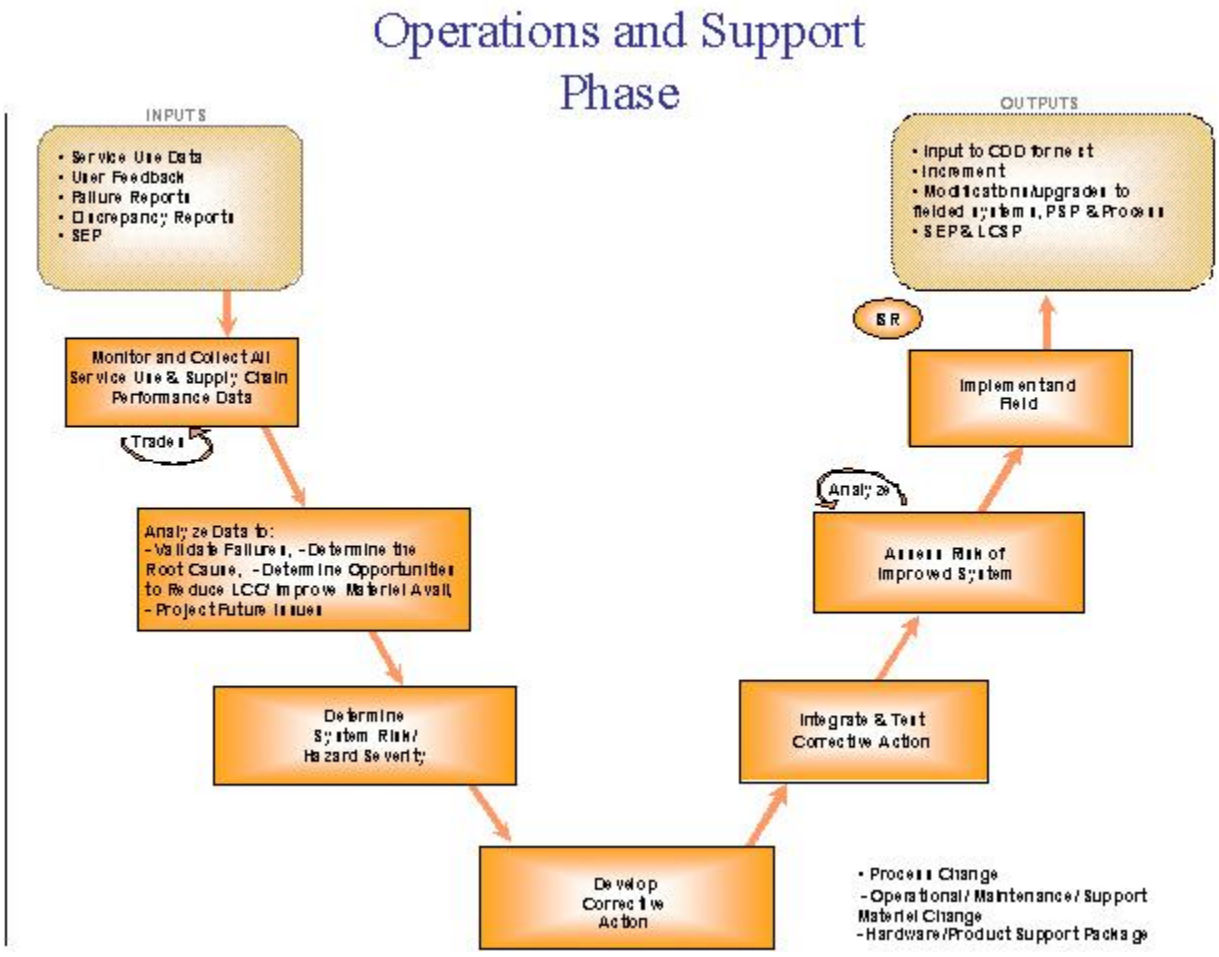


Figure 5.4.5.2.F1. System support implications in the Operations and Support Phase

5.4.5.2.1. Adjusting to meet User Needs

Under the total life-cycle systems management concept, the program manager continually assesses the system performance from the user's perspective. The PM should use existing reporting systems and user feedback to evaluate the fielded system, focusing on performance outcomes meaningful to the user. (If existing reporting systems do not provide sufficient information, the PM should augment existing reporting systems by collecting critical data required to assess performance and, where necessary, work with the DoD Components to add the capabilities to the existing reporting systems.) The data should be analyzed, comparing performance expectations against actual performance, root causes of problems identified, and corrective actions developed.

Potential corrective actions can be implemented through maintenance plan/requirement changes, process changes, modification of performance-based product support agreements, and/or design changes. The final decision for the corrective action selected will be determined by a balance between many factors, including but not limited to risk/safety, costs, schedule, user requirements and probability of success. (During this phase, the solution selected has a higher probability of success because more of the supportability analysis/RCM processes have the benefit of actuals, vice expectations, thereby reducing the amount of unknowns and eliminating many of the unknown-unknowns.) Regardless of the reason for the change (e.g., a required characteristic short fall, obsolescence, safety, changing user requirements or system design changes), the implementation/ fielding process will follow a tailored version of the Defense Acquisition Management System Framework.

5.4.5.2.2. In-Service Reviews (ISR)

The PM should conduct regularly scheduled In-Service Reviews (also know as Post IOC Reviews) with the users, assessing the current status, operational health and corrective actions to satisfy user operational needs based on user feedback and performance metrics. (See section 4.3.5.4 for additional information.) The ISR is a multi-disciplined product and process assessment to ensure the system is employed with well-understood and managed risk, so timely corrective actions can be taken. Leading into and during the reviews engineering, sustainment stakeholders (e.g., suppliers, representatives from primary supply chain providers, and the comptroller communities) and product support IPT members, as well as independent sustainment subject matter experts, should apply sound programmatic, systems engineering, and logistics management processes to:

- Assess product support performance against requirements and objectives. The focus should be on reliability, maintainability, and support problems (hardware and software) and their impact on safety and operational readiness. It should include an assessment of risk, readiness, and trends in a measurable form.
- Access the status of current system problems, solutions, and performance metrics. The metrics should include material reliability, material availability, mean down time, materiel ownership cost, and any additional useful sustainment metrics to substantiate in-service problems and budget priorities.

- Group system problems, safety, product support, and readiness issues by priority to form an integrated picture of in-service health, operational risk, system readiness, and future sustainment requirements. This information should be used to prioritize budget requirements (execution and out year) and future sustainment planning.
- Quantify and project system operational risk and system readiness levels based on current levels and current procurement, operations, and support budgets.
- Access the status of current initiatives and the program's responsiveness to meeting customer needs, including problem (discrepancy) report inflow, resolution rate, and trends.

The reviews should be conducted at defined intervals to identify needed revisions and corrections, and to allow for timely improvements in the strategies to meet performance requirements for materiel readiness. At least initially, the In-Service Reviews will focus on the product support package fielding including the product support providers performance against the PBAs and other requirements. Consequently, the reviews with the users and product support service providers should be on a semi-annual basis as the support plans are executed (including transition from organic to contract support and vice versa, if applicable). After the system has been fully deployed, the frequency of these reviews should then be based on system performance (including trends), the pace of technology, obsolescence issues, and safety. The program's In-Service Reviews should be used to prepare for the DoD Component level assessments or reviews.

5.4.5.2.3. Formal DoD Component Post Deployment Reviews

Program assessments encompass and evaluate supportability, logistics, readiness, and sustainment planning and are conducted by each DoD Component to help ensure a solid life-cycle product support program. Assessments independent of the program office are management practices that have proved to be useful in managing product support risks by providing an impartial evaluation of a program's product support and sustainment implementation. The DoD Components have independently established formal assessment processes in DoD Component specific policies and instructions. The process names vary, but all are intended to assist the PM in the successful execution of his/her total life-cycle management responsibilities. Links to key DoD Component assessment documents are provided in section 5.5 References.

The DoD Components conduct Post Deployment Reviews beginning at Initial Operational Capability (IOC) and then nominally every three to five years or when precipitated by changes in requirements/design or performance problems. These periodic assessments verify whether the fielded system continues to meet or exceed thresholds and objectives for cost, performance, and support parameters approved at the full rate production decision. In addition to comparing actual versus expected levels of performance and support, the reviews should at minimum include:

- Product Support Integrator/ Product Support Provider's performance, including effectiveness of sustained materiel readiness implementation
- Product improvements incorporated

- Configuration control

5.4.5.2.4. Life-Cycle Sustainment Plan

The LCSP should be used to help take the appropriate actions to meet total system availability requirements based on measured performance in the operational environment. (See figure 5.4.4.2.3.F1 for notional LCSP focus areas for this phase.) The plan documents the results of the stakeholder actions and projects outcomes expected based on the budget and real world conditions. The following aspects should be emphasized:

- Projected sustainment metric values over the FYDP reflecting the expected results of corrective actions under way
- Required and anticipated funding levels over the FYDP necessary to ensure acceptable reliability and availability rates and maintain mission capability against the relevant threats
- Management structure to detect sustainment problems, determine root causes and improve/ reduce the logistics footprint and improve materiel availability including resource levels
- Feedback mechanisms so actual effects or performance (including critical supply chain metrics (e.g., supply system or transportation response time, unit level skill level manning), overhauled/repaired equipment performance, diagnostic & predictive performance, corrosion effects) are fed back to the supply chain enabling additional proactive prevention/ correction steps taken. This should include the metrics being monitored and analyzed.

Once a program has been designated a "replaced system", a Replaced System Sustainment Plan will be generated which will require the program to work closely with the defense acquisition authority and the replacement system program manager. (See section 5.1.2.3)

5.4.5.3. Operations and Support Phase Results/Exit Criteria

Implementing the process depicted in **figure 5.4.5.2.F1** results in proactive support to the user focusing optimized resources to met operational needs. It can also result in new system requirements which would begin the **Life-Cycle Management System** process again.

The conclusion of this phase results in the disposal of the system following statutory regulations and policy. The PM should coordinate with DoD Component logistics activities and DLA, as appropriate, to identify and apply applicable demilitarization requirements necessary to eliminate the functional or military capabilities of assets (DoD 4140.1-R and DoD 4160.21-M-1). The PM should coordinate with DLA to determine property disposal requirements for system equipment, support assets, and by-products (DoD 4160.21-M).

5.4.5.4. Sustainment Considerations in the Operations and Support

Phase

DoD Instruction 5000.02, Enclosure 2, paragraph 8, includes "supply; maintenance; transportation; sustaining engineering; data management; configuration management; HSI; environment; safety (including explosives safety), and occupational health; protection of critical program information and anti-tamper provisions; supportability; and interoperability" within life-cycle sustainment. While not all of these elements are traditional logistics elements, all are important considerations for the PM to take into account in supporting the user. Key is ensuring the entire program is assessed and adjustments are made as needed, based on changing user requirements/needs or system design changes.

When assessing performance and revising agreements or support strategies, the process should encompass all configuration/block increments, and potential redesigns/ECPs to address changes required to address problems encountered in the operational environment. Emphasis should not only be on newly added support requirements, but also on addressing the support strategy in total across the entire platform and range of deployed configurations using the same analytical processes used in earlier phases.

The total life-cycle systems management and performance-based product support concept required by DoD 5000.01 necessitates that managing performance be focused on outcomes vs. segmented functional support organizational outputs. The PM is the focal point for ensuring that all program elements are considered and the respective stakeholders are engaged to support the user.

5.4.5.4.1. Sustainment Metrics

During this phase, the PM should measure, track and report the supply chain performance and its effectiveness, along with the sustainment metric drivers and the root cause of any performance shortfalls. Special emphasis should be placed on tracking the metrics for the drivers for the key enabler technologies that were developed for the system or are critical for achieving the required materiel availability.

5.4.5.5. Best Practices during Operations and Support

The following are important, but not the only, best practices to be used in this phase since the concepts previously spelled out still apply. In each case, the best practices involve the PM continually comparing performance against expectations, Using actual equipment and support performance data, to revise, correct and improve product support strategies to meet the users' requirements.

5.4.5.5.1. Continuous Process Improvement (CPI)

Often, due to revisions in funding, mission requirements, or other fact-of-life changes, logistics resources become out of balance or poorly synchronized. Therefore, PM efforts to achieve system availability while reducing costs should include periodic assessments and, where necessary, improvements of the support strategy and processes. While some system deficiencies can be addressed through system design, many can be more effectively resolved by adjusting the support strategy or processes. The continual application of supportability analysis, including condition based maintenance plus concepts, is an effective means of meeting evolving conditions and providing improved materiel availability.

Adjusting the maintenance requirements using RCM and CBM+ principles can be a very effective in optimizing the sustainment KPP and KSAs during the Operating and Support Phase. Additional approaches useful to the PM in balancing logistics resources, decreasing repair cycle times, and/or improving readiness/availability include:

- Application of Lean, Six Sigma and Theory of Constraints Concepts
- Updating the supply chain processes based on actuals. This can help balance logistics support through thorough review of readiness degraders, maintenance data, maintenance and support process implementation.
- Implementing properly incentivized performance-based agreements with support providers that encourage product support assessments and improvements based on comparisons between performance expectations against actual performance data

5.4.5.5.2. Supportability Analysis

During this phase, the supportability analysis continues to focus on design changes regardless of the need for the change (e.g., reliability shortfall, obsolescence issue, safety concern) and adjusting the support package to accommodate the changes. In this process, care should be given to ensure the analysis encompasses all previous configuration/block increments across the entire platform and range of deployed configurations. In doing this, the entire support strategy should be addressed to look for opportunities to reduce the logistics footprint and not just add on new sustainment requirements.

Supportability analysis should also be used to adjust the support package based on how it is performing. A wide range of changes (including moving between overhaul and repair, improving off equipment diagnostic capabilities, transitioning to a commercial supply chain management system, etc.) should be considered in determining the best solution. The ability to continually compare performance against expectations using actual equipment and support performance data to drive data analyses and a RCM decision analysis is more efficient and reduces risks.

In both cases, use data is monitored/collected and analyzed using FMECA. Any failure, maintenance or operational issues are verified and root causes, risk and severity are determined. An analysis should then be performed to determine if the most cost effective solution is a:

- Maintenance change (either a preventative maintenance task (including scheduled inspections) or, if it is a non critical failure, a corrective maintenance task. A Maintenance Plan analysis can help balance logistics support through thorough review of readiness degraders, maintenance data, maintenance procedures and commercial opportunities.
- Supply chain change
- Logistics element change
- Change in the operations or use of the system (including the timeframe and conditions under which the limitations will be have to remain in effect)
- Design change

In any proposed solution, the PM should work with the users to determine if the change and the timeframe are acceptable. Once the agreements have been reached, supportability analysis is used to adjust the appropriate logistics elements in the product support package.

5.4.5.5.3. Modeling and Simulation

During this phase M&S supports the program improvement efforts by analyzing the impact of proposed continuous process improvements, ECPs, and budget alternatives on the sustainment metrics as well as mission effectiveness. M&S can be used in assessing the alternatives affecting the design and deployment of both the end item and its support system. In addition, it can be used in a proactive mode to anticipate problems by taking use data and user feedback to:

- Project trends (with confidence levels) so actions are taken as conditions deteriorate to minimize adverse impacts on the users.
- Identify areas in the supply chain where performance is adversely affecting materiel availability, increasing ownership costs, or where there are opportunities for savings/improvements.
- Identify specific risk areas and ways to address/resolve root causes and reduce risk.

5.5. References

5.5.1. Handbooks and Guides

Performance-Based Life-Cycle Product Support Implementation Guide (Formally know as the Performance-Based Logistics: A Program Manager's Product Support Guide or the PBL Guide). This guide is a tool for Program Managers (PMs) and Product Support Managers as they design product support strategies for new programs or major modifications, or as they re-

engineer product support strategies for existing fielded systems. It presents a method for implementing a PBL support strategy. *Note, this guide is in the update process.*

Performance-Based Agreement Guidance. This guide and the Performance-Based Logistics section of Logistics Community of Practice (LOG CoP) provide guidance, explanations of Performance-Based Agreements, and related concepts for both Commercial and Organic PBAs. It includes sample Performance-Based Agreements, templates, contractual incentives, a Performance-Based Agreement Toolkit and other resources. It also includes An End to End Customer Support PBA template that provides a common framework and a checklist to consider when undertaking a performance-based type agreement that may involve one or more supply chain support services as well as PBA terms and definitions. Note, this guide is in the update process. *Note, this guide is in the update process.*

Designing and Assessing Supportability in DoD Weapon Systems: A Guide to Increased Reliability and Reduced Logistics Footprint (commonly referred to as the 'Supportability Guide'). This guide defines a framework for determining and continuously assessing system product support throughout the life cycle. It uses the Defense Acquisition Management Framework (as defined in DoD 5000 series policy) and systems engineering processes to define appropriate activities and required outputs throughout a system's life cycle to include those related to sustainment of fielded systems. *Note, this guide is in the update process.*

Operating and Support Cost-Estimating Guide. This guide and DoD Manual 5000.4, DoD Cost Analysis Guidance and Procedures provide procedures for life-cycle cost estimates. They explain the policies and procedures, focusing on the preparation, documentation, and presentation of cost estimates, and include and Operating and Support Cost element structure.

Diminishing Manufacturing Sources and Material Shortages (DMSMS) Guidebook. This guide consists of a compilation of the best practices for managing the risk of obsolescence. It identifies assorted measurement tools that may useful in analyzing and tracking the effectiveness of DMSMS programs.

CBM+ DoD Guidebook. This guide is an information reference as well as a tool to assist program and logistics managers with CBM+ project development, implementation, and execution. As a supplement to the CBM+ DoD Instruction, the Guidebook illustrates various complementary components of successful CBM+ implementation and describes management actions necessary to integrate technologies in order to increase reliability, availability, operational effectiveness, and maintenance efficiency.

5.5.2. Other References

The Acquisition Community Connection (ACC) and the Logistics Community of Practice (LOG CoP). The Acquisition Community Connection, sponsored by the Defense Acquisition University (DAU), is a tool to facilitate collaboration, sharing, and the transfer of knowledge across the DoD AT&L workforce. ACC is a collection of communities of practice centered on

different functional disciplines within the acquisition community. The Logistics Community of Practice, is one of the communities currently residing within the ACC framework. LOG CoP provides a number of resources for implementing life-cycle logistics. The community space also allows members to share (post to the website) their knowledge, lessons learned, and business case related material, so that the entire logistics community has access and can benefit.

Environment, Safety, and Occupational Health (ESOH). DoD ESOH Guidance for systems acquisition programs can be found in Chapter 4 Systems Engineering and in the ESOH Special Interest Area on the Acquisition Community.

The DoD Guide For Achieving Reliability, Availability, Maintainability (RAM). This document helps project managers and engineers to plan for and design RAM into systems. The guide focuses on what can be done in the systems engineering process to achieve effective levels of RAM, successfully demonstrate them during operational test and evaluation, and sustain them through the system's life cycle. It can be used to help capability document requirements writers and engineering organizations think through the top-level sustainment requirements for RAM early in the life cycle to ensure the system is sustainable and affordable throughout its life cycle.

The DoD Reliability, Availability, Maintainability & Cost (RAM-C) Rationale Report Manual. This manual describes the development of the RAM-C Rationale Report. It provides guidance in how to develop and document realistic sustainment Key Performance Parameter (KPP)/Key System Attribute (KSA) requirements and related supporting rationale. It addresses how the requirements must be measured and tested throughout the system life cycle as well as the processes that should be followed when developing the sustainment requirements.

DoD Instruction 4151.20, Depot Maintenance Core Capabilities Determination Process. This instruction describes the policy, assigns responsibilities, and prescribes procedures to implement 10 USC 2464 and DoD Directive 4151.18. It identifies the methodology to be used in determining the required core capabilities for depot maintenance and the associated workloads needed to sustain those capabilities.

DoD Instruction 5000.67, Prevention and Mitigation of Corrosion on DoD Military Equipment and Infrastructure. This instruction establishes policy, assigns responsibilities, prescribes procedures and provides guidance for the establishment and management of programs to prevent or mitigate corrosion of DoD military equipment and infrastructure.

CBM+ Continuous Learning Module (CLL029). The Condition Based Maintenance Plus (CBM+) module provides the learner with an overview and introduction to Depot Maintenance Management and Operations needed in DoD legacy systems. The module will cover DoD maintenance, CBM+ information and background, essential elements, CBM+ implementation, as well as managing initiatives and measuring success.

DEFENSE ACQUISITION GUIDEBOOK
Chapter 6 -- Human Systems Integration (HSI)

6.0. Overview

6.0. Overview

DoD acquisition policy requires optimizing total system performance and minimizing the cost of ownership through a "total system approach" to acquisition management (DoD Directive 5000.01).

6.0.1. Purpose

While Chapter 4 discusses systems engineering at large, this chapter specifically addresses the human systems elements of the systems engineering process. This chapter provides the Program Manager with the necessary background and understanding to design and develop systems that effectively and affordably integrate with human capabilities and limitations. It also makes the program manager aware of the staff resources available to assist in this endeavor.

6.0.2. Contents

This chapter has six major sections:

- Section 6.1 briefly reviews the total systems approach directed by DoD Directive 5000.01.

- Section 6.2 describes the importance of integration with respect to Human Systems Integration (HSI) implementation and its value in systems integration and risk management.
- Section 6.3 describes each of the domains of HSI: Manpower, Personnel, Training, Human Factors Engineering, Safety and Occupational Health, Survivability, and Habitability. Each of these sub-sections contains an overview of the domain, addresses domain requirements, and ends with a discussion of planning considerations, with one exception.
- Section 6.4 then follows with the implementation of HSI, to include formulation of the HSI strategy and the sequencing of expected HSI activities along the timeline of the Defense Acquisition Framework.
- Section 6.5 describes the human considerations associated with resource estimating and planning; it is the HSI complement to Chapter 3.
- The last section, Section 6.6, provides two reference lists for additional information.

6.1. Total System Approach

The total system includes not only the prime mission equipment, but also the people who operate, maintain, and support the system; the training and training devices; and the operational and support infrastructure. Human Systems Integration (HSI) practitioners assist program managers by focusing attention on the human part of the system and by integrating and inserting manpower, personnel, training, human factors engineering, environment, safety, occupational health, habitability, and survivability considerations into the Defense acquisition process. Consistent with DoD Instruction 5000.02, Enclosure 8, when addressing HSI, the program manager must focus on each of the "domains" of HSI. These domains are outlined and explained beginning in Section 6.3. The focus on the domains; however, should also include a comprehensive integration within and across these domains as outlined in Section 6.2.

6.2 HSI - Integration Focus

6.2 HSI - Integration Focus

The key to a successful HSI strategy is comprehensive integration across the HSI domains and also across other core acquisition and engineering processes. This integration is dependent on an accurate HSI plan and includes the comprehensive integration of requirements. The optimization of total system performance and determination of the most effective, efficient, and affordable design requires upfront requirements analyses. The HSI domains (manpower, personnel, training, environment, safety and occupational health, human factors engineering, survivability, and habitability) can and should be used to help determine and work the science and technology gaps

to address all aspects of the system (hardware, software, and human). The program manager should integrate system requirements for the HSI domains with each other, and also with the total system. As work is done to satisfy these requirements, it is vital that each HSI domain anticipate and respond to changes made by other domains or which may be made within other processes or imposed by other program constraints. These integration efforts should be reflected in updates to the requirements, objectives, and thresholds in the Capability Development Document.

In today's Joint environment, the integration across systems of systems is necessary to achieve a fully networked Joint war fighting capability. The warfighter requires a fully networked environment and must be able to operate efficiently and effectively across the continuum of systems from initial recognition of the opportunity to engage through to mission completion. To accomplish this, HSI should be considered through system-of-systems analysis, modeling, and testing to identify opportunities for integration, synchronization, collaboration, and coordination of capabilities to meet requirements. This may require a fully integrated investment strategy with joint sponsorship from the Materiel Development Decision on through the series of incremental developments.

Values for objectives and thresholds, and definitions for parameters contained in the capabilities documents, Manpower Estimate, Test and Evaluation Master Plan, and Acquisition Program Baseline, should be consistent. This ensures consistency and thorough integration of program interests throughout the acquisition process.

6.2.1. Integrated Product and Process Development (IPPD) and Integrated Product Teams (IPTs)

DoD acquisition policy stresses the importance of IPPD. IPPD is a management technique that integrates all acquisition activities starting with capabilities definition through systems engineering, production, fielding/deployment and operational support in order to optimize the design, manufacturing, business, and supportability processes. At the core of the IPPD technique are IPTs. Human Systems Integration (HSI) should be a key consideration during the formation of IPTs. HSI representatives should be included as members of systems engineering and design teams and other IPTs that deal with human-oriented acquisition issues or topics. The various HSI domain experts should have the opportunity to work in an integrated structure to comprehensively impact the system. Domain experts working separately and in different IPT structures may make significant changes / inputs to the system without fully appreciating changes made by other HSI domains participants in other IPTs or the effects their changes may have on other domains. This is particularly true when it comes to considerations such as systems safety, survivability, habitability, training and human factors engineering. Only by working closely together can the HSI practitioners bring an optimum set of human interfaces to the Systems Engineering and Systems Acquisition Processes. HSI participants assist in IPPD as part of the IPTs by ensuring the following:

- HSI parameters/requirements in the Initial Capabilities Document, Capability Development Document, and Capability Production Document are based upon and consistent with the user representative's strategic goals and strategies. These parameters/requirements are addressed throughout the acquisition process starting with technology development and continuing throughout engineering design, trade-off analysis, testing, fielding/deployment, and operational support;
- Safety and efficiency issues, identified in legacy systems and by review of design capability risks, are used to establish a preliminary hazard list for risk management and that the issues are effectively evaluated and managed throughout the system's life cycle at a management level consistent with the hazard;
- The factors, tools, methodologies, risk assessment/mitigations, and set of assumptions used by the acquisition community to assess manpower, personnel, and training requirements, measure human-in-the-loop system performance, and evaluate safety, occupational health hazards, survivability, and habitability are consistent with what the functional communities/user representatives use to evaluate performance and establish performance based metrics;
- The factors used by the acquisition community to develop cost estimates are consistent with the 1) manpower and personnel requirements reported in the Manpower Estimate; 2) training requirements reported in the DoD Component training plans; and 3) assessments of safety and health hazards documented in the Programmatic Environment, Safety, and Occupational Health Evaluation; and,
- The Manpower Estimates and training strategies reported during the acquisition milestone reviews are reflected in the manning documents, training plans, personnel rosters, and budget submissions when the systems are fielded.

6.2.2. HSI Strategy, Risk, and Risk Mitigation

The development of an HSI strategy should be initiated early in the acquisition process, when the need for a new capability or improvements to an existing capability is first established. To satisfy DoD Instruction 5000.02, the program manager should have a plan for HSI in place prior to entering Engineering and Manufacturing Development. The program manager should describe the technical and management approach for meeting HSI parameters in the capabilities documents, and identify and provide ways to manage any HSI-related cost, schedule, or performance issues that could adversely affect program execution.

When a defense system has complex human-systems interfaces; significant manpower or training costs; personnel concerns; or safety, health hazard, habitability, or survivability issues; the program manager should use the HSI plan to identify solutions. HSI risks and risk mitigation should be addressed in the acquisition strategy and the program manger's risk management program.

The HSI plan should address potential readiness or performance risks. For example, skill degradation can impact combat capability and readiness. The HSI plan should call for studies to identify operations that pose the highest risk of skill decay. When analysis indicates that the

combat capability of the system is tied to the operator's ability to perform discrete tasks that are easily degraded (such as those contained in a set of procedures), solutions such as embedded training should be considered to address the problem. Information overload and requirements for the warfighter to dynamically integrate data from multiple sources can result in degradation of situational awareness and overall readiness. Careful consideration of common user interfaces, composable information sources, and system workload management will mitigate this risk. An on-board "performance measurements capability" can also be developed to support immediate feedback to the operators/maintainers and possibly serve as a readiness measure to the unit commander. The lack of available ranges and other training facilities, when deployed, are issues that should be addressed. The increased use of mission rehearsal, as part of mission planning, and the preparation process and alternatives supporting mission rehearsal should be addressed in the HSI plan. Team skills training and joint battle space integration training should also be considered in the HSI plan and tied to readiness.

The program manager's Programmatic Environment, Safety, and Occupational Health (ESOH) Evaluation (PESHE) describes the strategy for integrating ESOH considerations into the systems engineering process and defines how PESHE is linked to the effort to integrate HSI considerations into systems engineering. The PESHE also describes how ESOH risks are managed and how ESOH and HSI efforts are integrated. It summarizes ESOH risk information (hazard identification, risk assessment, mitigation decisions, residual risk acceptance, and evaluation of mitigation effectiveness). The HSI Strategy should address the linkage between HSI and ESOH and how the program has been structured to avoid duplication of effort.

DoD Directive 5000.01 prescribes supportability comparable to cost, performance, and schedule in program decision-making. Program managers should establish a logistics support concept (e.g., two level, three level), training plans, and manpower and personnel concepts, that when taken together, provide for cost-effective, total, life-cycle support. MIL-HDBK-29612-1A, -2A, -3A, & -4A may be used as a guide for Instructional Systems Development/Systems Approach to the training and education process for the development of instructional materials. Manpower, personnel, training analyses should be tied to supportability analyses and should be addressed in the HSI plan.

Program risks related to cost, schedule, performance, supportability, and/or technology can negatively impact program affordability and supportability. The program manager should prepare a "fall-back" position to mitigate any such negative effect on HSI objectives. For example, if the proposed system design relies heavily on new technology or software to reduce operational or support manning requirements, the program manager should be prepared with design alternatives to mitigate the impact of technology or software that is not available when expected.

6.3. Human Systems Integration Domains

6.3.1. Manpower

6.3.1.1. Manpower Overview

Manpower factors are those job tasks, operation/maintenance rates, associated workload, and operational conditions (e.g., risk of hostile fire) that are used to determine the number and mix of military and DoD civilian manpower and contract support necessary to operate, maintain, support, and provide training for the system. Manpower officials contribute to the Defense acquisition process by ensuring that the program manager pursues engineering designs that optimize manpower and keep human resource costs at affordable levels (i.e., consistent with strategic manpower plans). Technology-based approaches used to reduce manpower requirements and control life-cycle costs should be identified in the capabilities documents early in the process. For example, material-handling equipment can be used to reduce labor-intensive material-handling operations and embedded training can be used to reduce the number of instructors.

6.3.1.2. Manpower Parameters/Requirements

DoD Directive 5000.01 directs the DoD Components to plan programs based on realistic projections of the dollars and manpower likely to be available in future years. Manpower goals and parameters should be based on manpower studies and analysis. These studies and analyses should ensure that design options that reduce workload and ensure program affordability are pursued, and that lower-priority design features do not take precedence. Throughout the system life cycle, program managers should strive to keep manpower and the associated ownership costs at desired/targeted levels. Program managers should also preserve future-year resources rather

than attempting to compete for additional funding later to address Manpower, Personnel or associated Training issues.

When there are Congressional or Administrative caps placed on military end strengths, the introduction of a new system or capability will require compensating reductions (trade-offs) elsewhere in the force structure or in the Individuals Account. Manpower officials should identify areas for offsets, or "bill-payers," for the new system and establish constraints based on available resources. If the new system replaces a system in the inventory, manpower officials should determine whether the constraints placed on the predecessor system also apply to the new system. They should consider the priority of the new system and determine if either additional resources will be provided, or if more stringent constraints will apply. Manpower authorities should consider the availability of resources over the life of the program and weigh competing priorities when establishing manpower constraints for acquisition programs. Reviews should account for all military and civilian manpower and contract support needed to operate, maintain, support, and provide training for the system over the entire life of the program.

Manpower can be a major determinant of program cost and affordability. In translating user requirements into a Defense Acquisition Program and its associated program documents, both the Program Managers and HSI practitioners should ensure that the requirements documents provide sufficient guidance to accurately move forward. The Capability Development Document (CDD) should identify any manpower constraints that, if exceeded, would require the Department to reconsider the utility of the program. The CDD should specify the expected location of the system on the battlefield and the expected operational conditions (e.g., a high [or low] likelihood of hostile fire or collateral damage). These specifications affect early cost, manpower mix, training, personnel, and survivability requirements. Absent this guidance, further clarification should be requested from the users.

The CDD should establish manpower parameters (objectives and thresholds) consistent with existing departmental constraints. If the program is manpower intensive, it may be prudent to establish a manpower Key Performance Parameter (KPP) early in the acquisition process. Setting a KPP will ensure the system fits within manpower parameters established by the Department, that agreed-upon resource thresholds are not exceeded, and that the system will not require additional resources from higher priority programs later in the acquisition process. A KPP should only be established if the adverse manpower effect of exceeding the KPP outweighs the overall benefits of the new capability. In all cases, manpower constraints and KPPs must be defendable and commensurate with the priority and utility of the new capability. Program Managers and HSI practitioners should work closely with the users and the sponsoring organization to ensure agreement on the appropriate parameters.

The CDD should also address specific, scenario-based, factors that affect manpower, such as surge requirements, environmental conditions (e.g., arctic or desert conditions), and expected duration of the conflict. These factors are capability-related and directly affect the ability of the commander to sustain operations in a protracted conflict.

6.3.1.3. Manpower Planning

Manpower analysts determine the number of people required, authorized, and available to operate, maintain, support, and provide training for the system. Manpower requirements are based on the range of operations during peacetime, low intensity conflict, and wartime. They should consider continuous, sustained operations and required surge capability. The resulting Manpower Estimate accounts for all military (Active Reserve, and Guard), DoD civilian (U.S. and foreign national), and contract support manpower.

DoD Instruction 5000.02 requires the program manager to work with the manpower community to determine the most efficient and cost-effective mix of DoD manpower and contract support, and identify any issues (e.g., resource shortfalls) that could impact the program manager's ability to execute the program. This collaboration be conducted within the Human Systems Integration (HSI) framework to ensure integration with the other HSI domains. The HSI lead for a program / project should be able to draw expertise from the manpower community to provide program assistance. Generally, the decision to use DoD civilians and contract labor in theater during a conflict where there is a high likelihood of hostile fire or collateral damage is made on an exception basis. In all cases, risk reduction should take precedence over cost savings. Additionally, the program manager shall consult with the manpower community in advance of contracting for operational support services to ensure that sufficient workload is retained in-house to adequately provide for career progression, sea-to-shore and overseas rotation, and combat augmentation. The program manager should also ensure that inherently governmental and exempted commercial functions are not contracted. These determinations shall be based on current Workforce Mix Guidance (DoD Instruction 1100.22).

Consistent with sections E1.1.4 and E1.1.29 of DoD Directive 5000.01, the program manager must evaluate the manpower required and/or available to support a new system and consider manpower constraints when establishing contract specifications to ensure that the human resource demands of the system do not exceed the projected supply. The assessment must determine whether the new system will require a higher, lower, or equal number of personnel than the predecessor system, and whether the distribution of ranks/grade will change. Critical manpower constraints must be identified in the Capability Development Document to ensure that manpower requirements remain within DoD Component end-strength constraints. If sufficient end-strength is not available, a request for an increase in authorizations should be submitted and approved as part of the trade-off process.

When assessing manpower, the system designers should look at labor-intensive (high-driver) tasks. These tasks might result from hardware or software interface design problems. These high-driver tasks can sometimes be eliminated during engineering design by increasing equipment or software performance. Based on a top-down functional analysis, an assessment should be conducted to determine which functions should be automated, eliminated, consolidated, or simplified to keep the manpower numbers within constraints.

Manpower requirements should be based on task analyses that are conducted during the functional allocation process and consider all factors including fatigue; cognitive, physical, sensory overload; environmental conditions (e.g., heat/cold), and reduced visibility. Additionally, manpower must be considered in conjunction with personnel capabilities, training, and human factors engineering trade-offs.

Tasks and workload for individual systems, systems-of-systems, and families-of-systems should be reviewed together to identify commonalities, merge operations, and avoid duplication. The cumulative effects of system-of-system, family-of-systems and related system integration should be considered when developing manpower estimates.

When reviewing support activities, the program manager should work with manpower and functional representatives to identify process improvements, design options, or other initiatives to reduce manpower requirements, improve the efficiency or effectiveness of support services, or enhance the cross-functional integration of support activities.

The support strategy should document the approach used to provide for the most efficient and cost-effective mix of manpower and contract support and identify any cost, schedule, or performance issues, uncompleted studies that could impact the program manager's ability to execute the program.

6.3.2. Personnel

6.3.2.1. Personnel Overview

6.3.2.2. Personnel Parameters/Requirements

6.3.2.3. Personnel Planning

6.3.2.1. Personnel Overview

Personnel factors are those human aptitudes (i.e., cognitive, physical, and sensory capabilities), knowledge, skills, abilities, and experience levels that are needed to properly perform job tasks. Personnel factors are used to develop the military occupational specialties (or equivalent DoD Component personnel system classifications) and civilian job series of system operators, maintainers, trainers, and support personnel. Personnel officials contribute to the Defense acquisition process by ensuring that the program manager pursues engineering designs that minimize personnel requirements, and keep the human aptitudes necessary for operation and maintenance of the equipment at levels consistent with what will be available in the user population at the time the system is fielded.

6.3.2.2. Personnel Parameters/Requirements

DoD Instruction 5000.02 requires the program manager to work with the personnel community to define the performance characteristics of the user population, or "target audience," early in the acquisition process. The program manager should work with the personnel community to establish a Target Audience Description (TAD) that identifies the cognitive, physical, and sensory abilities-i.e., capabilities and limitations, of the operators, maintainers, and support personnel expected to be in place at the time the system is fielded. When establishing the TAD, Human Systems Integration (HSI) practitioners should verify whether there are any recruitment or retention trends that could significantly alter the characteristics of the user population over the life of the system. Additionally, HSI analysts should consult with the personnel community and verify whether there are new personnel policies that could significantly alter the scope of the user population (e.g., policy changes governing women in combat significantly changed the anthropometric requirements for occupational specialties).

Per DoD Instruction 5000.02, to the extent possible--systems shall not be designed to require cognitive, physical, or sensory skills beyond those found in the specified user population. During functional analysis and allocation, tasks should be allocated to the human component consistent with the human attributes (i.e., capabilities and limitations) of the user population to ensure compatibility, interoperability, and integration of all functional and physical interfaces. Personnel requirements should be established consistent with the knowledge, skills, and abilities (KSAs) of the user population expected to be in place at the time the system is fielded and over the life of the program. Personnel requirements are usually stated as a percentage of the population. For example, the Capability Development Document might require "physically accommodating the central 90% of the target audience." Setting specific, quantifiable, personnel requirements in the Capability Development Document assists establishment of test criterion in the Test and Evaluation Master Plan.

6.3.2.3. Personnel Planning

Personnel capabilities are normally reflected as knowledge, skills, abilities (KSAs), and other characteristics. The availability of personnel and their KSAs should be identified early in the acquisition process. The DoD Components have a limited inventory of personnel available, each with a finite set of cognitive and psychomotor abilities. This could affect specific system thresholds.

The program manager should use the target audience description (TAD) as a baseline for personnel requirements assessment. The TAD should include information such as inventory; force structure; standards of grade authorizations; personnel classification (e.g., Military Occupational Code / Navy Enlisted Classification) description; biographical information; anthropometric data; physical qualifications; aptitude descriptions as measured by the Armed Services Vocational Aptitude Battery (ASVAB)); task performance information; skill grade authorization; Military Physical Profile Serial System (PULHES); security clearance; and reading grade level.

The program manager should assess and compare the cognitive and physical demands of the projected system against the projected personnel supply. The program manager should also determine the physical limitations of the target audience (e.g., color vision, acuity, and hearing). The program manager should identify any shortfalls highlighted by these studies.

The program manager should determine if the new system contains any aptitude-sensitive critical tasks. If so, the program manager should determine if it is likely that personnel in the target audience can perform the critical tasks of the job.

The program manager should consider personnel factors such as availability, recruitment, skill identifiers, promotion, and assignment. The program manager should consider the impact on recruiting, retention, promotions, and career progression when establishing program costs, and should assess these factors during trade-off analyses.

The program manager should use a truly representative sample of the target population during Test and Evaluation (T&E) to get an accurate measure of system performance. A representative sample during T&E will help identify aptitude constraints that affect system use.

Individual system and platform personnel requirements should be developed in close collaboration with related systems throughout the Department and in various phases of the acquisition process to identify commonalities, merge requirements, and avoid duplication. The program manager should consider the cumulative effects of system-of-systems, family-of-systems, and related systems integration in the development of personnel requirements

Consistent with DoD Instruction 5000.02, Enclosure 8, the program manager should summarize major personnel initiatives that are necessary to achieve readiness or rotation objectives or to reduce manpower or training costs, when developing the acquisition strategy. The acquisition strategy and Life-Cycle Sustainment Plan should address modifications to the knowledge, skills, and abilities of military occupational specialties for system operators, maintainers, or support personnel if the modifications have cost or schedule issues that could adversely impact program execution. The program manager should also address actions to combine, modify, or establish new military occupational specialties or additional skill indicators, or issues relating to hard-to-fill occupations if they impact the program manager's ability to execute the program.

6.3.3. Training

6.3.3.1. Training Overview

Training is the learning process by which personnel individually or collectively acquire or enhance pre-determined job-relevant knowledge, skills, and abilities by developing their cognitive, physical, sensory, and team dynamic abilities. The "training/instructional system" integrates training concepts and strategies and elements of logistic support to satisfy personnel performance levels required to operate, maintain, and support the systems. It includes the "tools" used to provide learning experiences such as computer-based interactive courseware, simulators, and actual equipment (including embedded training capabilities on actual equipment), job performance aids, and Interactive Electronic Technical Manuals.

6.3.3.2. Training Parameters/Requirements

When developing the training/instructional system, the program manager should employ transformational training concepts, strategies, and tools such as computer based and interactive courseware, simulators, and embedded training consistent with the strategy, goals and objectives of the Strategic Plan for Transforming DoD Training and the Training Transformation Implementation Plan. In addition, the program should address the requirement for a systems training key performance parameter as described in the JCIDS Manual.

The Department's vision for Training Transformation is to provide dynamic, capabilities-based training in support of national security requirements across the full spectrum of service, joint, interagency, intergovernmental, and multinational operations. This new approach emphasizes the mission requirements of the combatant commanders (COCOM). The COCOMs are the customers. The intent is to design systems and structure acquisition programs focused on the training needs of the COCOM. The desired outcome is to fully support COCOM requirements, missions, and capabilities, while preserving the ability of the DoD Components to train for their core competencies. The Under Secretary of Defense for Personnel and Readiness (USD(P&R)), as a member of the Defense Acquisition Board (DAB), assesses the ability of the acquisition program to support the Military Departments, COCOMs, and other DoD Components.

"Training," in this context, includes training, education, and job-performance aiding. Joint training should be able to support a broad range of roles and responsibilities in military, multinational, interagency, and intergovernmental contexts, and the Department of Defense must provide such training to be truly flexible and operationally effective. Training readiness will be assessed and reported, not only in the traditional joint context, but also in view of this broader range of "joint" operations. Joint training and education will be recast as components of lifelong learning and made available to the Total Force-active, reserve, DoD civilians and contract support. The Department will expand efforts to develop officers well versed in joint operational art. The interfaces between training systems and the acquisition process will be strengthened. The USD(P&R), as a member of the DAB, assesses an acquisition program's ability to support the COCOM's and DoD Components' capabilities to provide Human Systems Integration as an integral part of an acquisition program.

The program manager should summarize major elements of the training plan in the Support Strategy. This should include logistics support planning for training, training equipment and training device acquisitions and installations.

A Special Note on Embedded Training. Both the sponsor and the program manager should give careful consideration and priority to the use of embedded training as defined in DoD Directive 1322.18: "Capabilities built into, strapped onto, or plugged into operational materiel systems to train, sustain, and enhance individual and crew skill proficiencies necessary to operate and maintain the equipment." The sponsor's decisions to use embedded training should be made very early in the capabilities determination process. Analysis should be conducted to compare the embedded training with more traditional training media (e.g., simulator based training, traditional classroom instruction, and/or maneuver training) for consideration of a system's Total Operating Cost. The analysis should compare the costs and the impact of embedded training (e.g., training operators and maintenance personnel on site compared to off station travel to a temporary duty location for training). It should also compare the learning time and level of effectiveness (e.g., higher "kill" rates and improved maintenance times) achieved by embedded training. When making decisions about whether to rely exclusively on embedded training, analysis should be conducted to determine the timely availability of new equipment to all categories of trainees (e.g., Reserve and Active Component units or individual members). For instance, a National Guard tank battalion that stores and maintains its tanks at a central maintenance/training facility may find it more cost effective to rely on mobile simulator assets to train combat tasks rather than transporting its troops to the training facility during drill weekends. A job aid for embedded training costing and effectiveness analyses is: "A Guide for Early Embedded Training Decisions," U.S. Army Research Institute for the Behavioral and Social Sciences Research Product 96-06.

6.3.3.3. Training Planning

This section will prepare the Program Manager to understand training capabilities as an integral part of the Joint Capabilities Integration and Development System (JCIDS) and, with assistance of the training community, translate those capabilities into system design features.

First, the JCIDS process should address joint training parameters for military (Active, Reserve, and Guard) civilian and contractor support personnel who will operate, maintain, and support the system. Training programs should employ a cost-effective solution, consisting of a blend of capabilities that use existing training programs and introduces new performance-based training innovations. This may include requirements for school and unit training, as well as new equipment training, or sustainment training. This also may include requirements for instructor and key personnel training and new equipment training teams.

Training should be considered early in the capabilities development process beginning with the analyses that supports development of the Initial Capabilities Document and continues with development of the Capability Development Document. It should also be considered in

collaboration with each of the other Human Systems Integration (HSI) domains in order to capture the full extent of the human integration issues that need to be accommodated.

The Capability Development Document should discuss the specific system training requirements and the training Key Performance Parameter:

- Allow for interactions between platforms or units (e.g., through advanced simulation and virtual exercises) and provide training realism to include threats (e.g., virtual and surrogate), a realistic electronic warfare environment, communications, and weapons.
- Embedded training capabilities that do not degrade system performance below threshold values nor degrade the maintainability or component life of the system.
- That Initial Operational Capability is attained and that training capabilities are embedded and met by Initial Operational Capability.
- An embedded performance measurement capability to support immediate feedback to the operators/maintainers and possibly to serve as a readiness measure for the unit commander.
- Training logistics necessary to support the training concept (e.g., requirements for new or upgrades to existing training facilities).

The training community should be specific in translating capabilities into system requirements. They should also set training resource constraints. These capabilities and constraints can be facilitated and worked through system integration efforts in several of the other HSI domains. Examples are:

- The training community should consider whether the system be designed with a mode of operation that allows operators to train interactively on a continuous basis, even when deployed in remote / austere locations.
- The training community should consider whether the system be capable of exhibiting fault conditions for a specified set of failures to allow rehearsal of repair procedures for isolating faults or require that the system be capable of interconnecting with other (specific) embedded trainers in both static and employed conditions.
- The training community should consider whether embedded training capabilities allow enhancements to live maneuvers such that a realistic spectrum of threats is encountered (e.g., synthetic radar warnings generated during flight).
- The training community should consider whether the integrated training system be fully tested, validated, verified, and ready for training at the training base as criteria for declaring Initial Operational Capability.

From the earliest stages of development and as the system matures, the program manager should emphasize training requirements that enhance the user's capabilities, improve readiness, and reduce individual and collective training costs over the life of the system. This may include requirements for expert systems, intelligent tutors, embedded diagnostics, virtual environments, and embedded training capabilities. Examples of training that enhances user's capabilities follow:

- Interactive electronic technical manuals provide a training forum that can significantly reduce schoolhouse training and may require lower skill levels for maintenance personnel while actually improving their capability to maintain an operational system;
- Requirements for an embedded just-in-time mission rehearsal capability supported by the latest intelligence information and an integrated global training system/network that allows team training and participation in large scale mission rehearsal exercises can be used to improve readiness.

In all cases, the paramount goal of the training/instructional system should be to develop and sustain a ready, well-trained individual/unit, while giving strong consideration to options that can reduce life-cycle costs and provide positive contributions to the joint context of a system, where appropriate.

Training devices and simulators are systems that, in some cases, may qualify for their own set of HSI requirements. For instance, the training community may require the following attributes of a training simulator:

- Accommodate "the central 90 percent of the male and female population on critical body dimensions;"
- Not increase manpower requirements and considerations of reductions in manpower requirements;
- Consider reduced skill sets to maintain because of embedded instrumentation;
- Be High Level Architecture compliant;
- Be Sharable Content Object Reference Model compliant;
- Be Test and Training Enabling Architecture (overview) compliant;
- Use reusable simulation objects.

6.3.4. Human Factors Engineering (HFE)

6.3.4.6. Life-Cycle Sustainment Plan and Acquisition Strategy

6.3.4.1. Mandatory Guidance

In accordance with DoD Instruction 5000.02, the program manager shall employ human factors engineering to design systems that require minimal manpower; provide effective training; can be operated and maintained by users; and are suitable (habitable and safe with minimal environmental and occupational health hazards) and survivable (for both the crew and equipment).

> *The PM shall take steps (e.g., contract deliverables and Government/contractor IPT teams) to ensure ergonomics, human factors engineering, and cognitive engineering is employed during systems engineering over the life of the program to provide for effective human-machine interfaces and to meet HSI requirements. Where practicable and cost effective, system designs shall minimize or eliminate system characteristics that require excessive cognitive, physical, or sensory skills; entail extensive training or workload-intensive tasks; result in mission-critical errors; or produce safety or health hazards.*

The human factors that need to be considered in the integration are discussed below:

6.3.4.2. Overview

Human factors are the end-user cognitive, physical, sensory, and team dynamic abilities required to perform system operational, maintenance, and support job tasks. Human factors engineers contribute to the acquisition process by ensuring that the program manager provides for the effective utilization of personnel by designing systems that capitalize on and do not exceed the abilities (cognitive, physical, sensory, and team dynamic) of the user population. The human factors engineering community works to integrate the human characteristics of the user population into the system definition, design, development, and evaluation processes to optimize human-machine performance for operation, maintenance, and sustainment of the system.

Human factors engineering is primarily concerned with designing human-machine interfaces consistent with the physical, cognitive, and sensory abilities of the user population. Human-machine interfaces include:

- Functional interfaces (functions and tasks, and allocation of functions to human performance or automation);
- Informational interfaces (information and characteristics of information that provide the human with the knowledge, understanding and awareness of what is happening in the tactical environment and in the system);

- Environmental interfaces (the natural and artificial environments, environmental controls, and facility design);
- Cooperational interfaces (provisions for team performance, cooperation, collaboration, and communication among team members and with other personnel);
- Organizational interfaces (job design, management structure, command authority, policies and regulations that impact behavior);
- Operational interfaces (aspects of a system that support successful operation of the system such as procedures, documentation, workloads, job aids);
- Cognitive interfaces (decision rules, decision support systems, provision for maintaining situational awareness, mental models of the tactical environment, provisions for knowledge generation, cognitive skills and attitudes, memory aids); and,
- Physical interfaces (hardware and software elements designed to enable and facilitate effective and safe human performance such as controls, displays, workstations, worksites, accesses, labels and markings, structures, steps and ladders, handholds, maintenance provisions, etc,).

6.3.4.3. Parameters/Requirements

Human factors requirements, objectives, and thresholds should be derived from each of the Human Systems Integration (HSI) domains and should provide for the effective utilization of personnel through the accommodation of the cognitive, physical, and sensory characteristics that directly enhance or constrain system performance. In many cases, the interface design limitation may require tradeoffs in several of the other domains and vice, versa.

Cognitive requirements address the human's capability to evaluate and process information. Requirements are typically stated in terms of response times and are typically established to avoid excessive cognitive workload. Operations that entail a high number of complex tasks in a short time period can result in cognitive overload and safety hazards. The Capability Development Document should specify whether there are human-in-the-loop requirements. This could include requirements for "human in control," "manual override," or "completely autonomous operations." Knowledge, skills and abilities for operators, maintainers and other support personnel continuously change with the increasing complexity of emerging systems. These requirements should be cross correlated with each of the HSI domains.

Physical requirements are typically stated as anthropometric (measurements of the human body), strength, and weight factors. Physical requirements are often tied to human performance, safety, and occupational health concerns. To ensure the average user can operate, maintain, and support the system, requirements should be stated in terms of the user population. For instance, when the user requires a weapon that is "one-man portable," weight thresholds and objectives should be based on strength limitations of the user population and other related factors (e.g., the weight of other gear and equipment and the operational environment). For example, it may be appropriate to require that "the system be capable of being physically maintained by 90% of both the male and female population, inclusive of battle dress, or arctic and Mission Oriented Protective Postures-Level 4 protective garments inside the cab," or that "the crew station

physically accommodate 90% of the female/male population, defined by current anthropometric data, for accomplishment of the full range of mission functions."

Sensory requirements are typically stated as visual, olfactory (smell), or hearing factors. The Capability Development Document should identify operational considerations that affect sensory processes. For example, systems may need to operate in noisy environments where weapons are being fired or on an overcast moonless night with no auxiliary illumination. Visual acuity or other sensory requirements may limit the target audience for certain specialties.

6.3.4.4. Application of Human Factors Engineering (HFE)

HFE plays an important role in each phase of the acquisition cycle, to include requirements development, system definition, design, development, evaluation, and system support for reliability and maintainability in the field. To realize the potential of HFE contributions, HFE must be incorporated into the design process at the earliest stages of the acquisition process (i.e., during the Materiel Solution Analysis and Technology Development phases). It should be supported by inputs from the other Human Systems Integration (HSI) domains as well as the other Systems Engineering processes. The right decisions about the human-machine interfaces early in the design process will optimize human and hence, total systems performance. HFE participation continues to each succeeding acquisition phase, continuing to work tradeoffs based on inputs from the other HSI domains and the hardware and software designs / adaptations. The HFE practitioners provide expertise that includes design criteria, analysis and modeling tools, and measurement methods that will help the program office design systems that are operationally suitable, safe, survivable, effective, usable, and cost-effective. In any system acquisition process, it is important to recognize the differences between the competencies (skills and knowledge) required for the various warfighters. Application of HFE processes will lead to an understanding of the competencies needed for the job, and help identify if requirements for knowledge, skills, and abilities (KSAs) exceed what the user can provide and whether the deficiency will lead to a training or operational problem. HFE tools and techniques can be used to identify the KSAs of the target audience and account for different classes and levels of users and the need for various types of information products, training, training systems and other aids. While it is critical to understand the information processing and net-centric requirements of the system, it is equally important to understand the factors affecting format and display of the data presented to the user to avoid cognitive overload. This applies equally to the system being designed as well as to the systems which will interface with the system. The system should not place undue workload or other stress on systems with which it must interface.

6.3.4.5. General Guidelines

Human Factors Engineering (HFE) should be applied during development and acquisition of military systems, equipment, and facilities to integrate personnel effectively into the design of the system. An HFE effort should be provided to: (a) develop or improve all human interfaces of the system; (b) achieve required effectiveness of human performance during system operation,

maintenance, support, control, and transport; and (c) make economical demands upon personnel resources, skills, training, and costs. The HFE effort should be well integrated with the other Human Systems Integration domain participation, and should include, but not necessarily be limited to, active participation in the following three major interrelated areas of system development

6.3.4.5.1. Analysis

Identify the functions that must be performed by the system in achieving its mission objectives and analyze them to determine the best allocation to personnel, equipment, software, or combinations thereof. Allocated functions should be further dissected to define the specific tasks that must be performed to accomplish the functions. Each task should be analyzed to determine the human performance parameters; the system, equipment, and software capabilities; and the operational / environmental conditions under which the tasks will be conducted. Task parameters should be quantified where possible, and should be expressed in a form that permits effectiveness studies of the human-system interfaces in relation to the total system operation. Human Factors Engineering high-risk areas should be identified as part of the analysis. Task analysis should include maintenance and sustainment functions performed by crew and support facilities. Analyses should be updated as required to remain current with the design effort.

6.3.4.5.2. Design and Development

Human Factors Engineering (HFE) should be applied to the design and development of the system equipment, software, procedures, work environments, and facilities associated with all functions requiring personnel interaction. This HFE effort should convert the mission, system, and task analysis data into a detailed design and development plan to create a human-system interfaces that will operate within human performance capabilities, facilitate / optimize human performance in meeting system functional requirements, and accomplish the mission objectives.

6.3.4.5.3. Test and Evaluation (T&E)

Human Factors Engineering (HFE) and the evaluation of all human interfaces should be integrated into engineering design and development tests, contractor demonstrations, flight tests, acceptance tests, other development tests and operational testing. Compliance with human interface requirements should be tested as early as possible. T&E should include evaluation of maintenance and sustainment activities and evaluation of the dimensions and configuration of the environment relative to criteria for HFE and each of the other Human Systems Integration domains. Findings from design reviews, modeling, simulations, demonstrations, and other early engineering tests should be used in planning and conducting later tests. Test planning should be directed toward verifying that the system can be operated, maintained, supported, and controlled by user personnel in its intended operational environment with the intended training. Test planning should also consider data needed or provided by operational test and evaluation. (See section 9.4.5).

6.3.4.6. Life-Cycle Sustainment Plan and Acquisition Strategy

The program manager should summarize the steps planned to be taken (e.g., contract deliverables) to ensure human factors engineering (HFE)/cognitive engineering is employed during systems engineering over the life of the program to provide for effective human-machine interfaces and meet HFE and other Human Systems Integration requirements.

6.3.5. Environment, Safety and Occupational Health (ESOH)

6.3.5.1. Environment, Safety and Occupational Health (ESOH) Overview

Each of the various military departments / services treat the three Human Systems Integration (HSI) domains of Environment, Safety, and Occupational Health differently, based on oversight and reporting responsibility within each of the services. DoD ESOH Guidance for systems acquisition programs can be found in Chapter 4, Systems Engineering, section 4.4, and in the ESOH Special Interest Area on the Acquisition Community Connection. What is important to the HSI practitioner and the systems engineer is that these three domains are of vital importance to the HSI effort and must be integrated within the HSI effort. While the ESOH communities have unique reporting requirements that trace to National level mandates, the importance of integrating these domains in the HSI construct cannot be overemphasized. The human aspect brings a host of issues to a system that must be accommodated in each of these three areas and they must each be considered in consonance with the other HSI domains. How they are considered in an integrated manner is left to the Program Manager and Systems Engineering.

Environment includes the conditions in and around the system and the operational context within which the system will be operated and supported. This "environment" affects the human's ability to function as a part of the system. Safety factors consist of those system design characteristics that serve to minimize the potential for mishaps causing death or injury to operators and maintainers or threaten the survival and/or operation of the system. Prevalent issues include factors that threaten the safe operation and/or survival of the platform; walking and working surfaces including work at heights; pressure extremes; and control of hazardous energy releases such as mechanical, electrical, fluids under pressure, ionizing or non-ionizing radiation (often

referred to as "lock-out/tag-out"), fire, and explosions. Occupational health factors are those system design features that serve to minimize the risk of injury, acute or chronic illness, or disability; and/or reduce job performance of personnel who operate, maintain, or support the system. Prevalent issues include noise, chemical safety, atmospheric hazards (including those associated with confined space entry and oxygen deficiency), vibration, ionizing and non-ionizing radiation, and human factors issues that can create chronic disease and discomfort such as repetitive motion diseases. Many occupational health problems, particularly noise and chemical management, overlap with environmental impacts. Human factors stresses that create risk of chronic disease and discomfort overlap with occupational health considerations.

6.3.5.2. Environment, Safety and Occupational Health (ESOH) Hazard Parameters/Requirements

Environment, safety and health hazard parameters should address all activities inherent to the life cycle of the system, including test activity, operations, support, maintenance, and final demilitarization and disposal. Environment, safety and health hazard requirements should be stated in measurable terms, whenever possible. For example, it may be appropriate to establish thresholds for the maximum level of acoustic noise, vibration, acceleration shock, blast, temperature or humidity, or impact forces etc., or "safeguards against uncontrolled variability beyond specified safe limits," where the Capability Production Document specifies the "safe limits." Safety and health hazard requirements often stem from human factor issues and are typically based on lessons learned from comparable or predecessor systems. For example, both physical dimensions and weight are critical safety requirements for the accommodation of pilots in ejection seat designs. Environment, safety and health hazard thresholds are often justified in terms of human performance requirements, because, for example, extreme temperature and humidity can degrade job performance and lead to frequent or critical errors. Another methodology for specifying safety and health requirements is to specify the allowable level of residual risk as defined in MIL-STD-882D, "DoD Standard Practice for System Safety," for example, "There shall be no high or serious residual risks present in the system."

6.3.5.3. Environment, Safety and Occupational Health (ESOH) Planning

6.2.5.3.1. Programmatic Environment, Safety, and Occupational Health (ESOH) Evaluation (PESHE

The Human Systems Integration Strategy should recognize the appropriate timing for the PESHE and define how the program intends to ensure the effective and efficient flow of information to and from the ESOH domain experts to work the integration of environment, safety and health considerations into the systems engineering process and all its required products.

6.3.5.3.2. Health Hazard Analysis (HHA)

During early stages of the acquisition process, sufficient information may not always be available to develop a complete HHA. As additional information becomes available, the initial analyses are refined and updated to identify health hazards, assess the risks, and determine how to mitigate the risks, formally accept the residual risks, and monitor the effectiveness of the mitigation measures. The health hazard risk information is documented in the PESHE. Health hazard assessments should include cost avoidance figures to support trade-off analysis. There are nine health hazard issues typically addressed in a health hazard analysis (HHA):

- **Acoustical Energy.** The potential energy that transmits through the air and interacts with the body to cause hearing loss or damage to internal organs.
- **Biological Substances.**
- **Chemical Substances.** The hazards from excessive airborne concentrations of toxic materials contracted through inhalation, ingestion, and skin or eye contract.
- **Oxygen Deficiency**. The displacement of atmospheric oxygen from enclosed spaces or at high altitudes.
- **Radiation Energy. Ionizing:** The radiation causing ionization when interfacing with living or inanimate mater. Non-ionizing: The emissions from the electromagnetic spectrum with insufficient energy to produce ionizing of molecules.
- **Shock.** The mechanical impulse or impact on an individual from the acceleration or deceleration of a medium.
- **Temperature Extremes and Humidity.** The human health effects associated with high or low temperatures, sometimes exacerbated by the use of a materiel system.
- **Trauma. Physical:** The impact to the eyes or body surface by a sharp or blunt object. Musculoskeletal: The effects to the system while lifting heavy objects.
- **Vibration.** The contact of a mechanically oscillating surface with the human body.

6.3.6. Survivability

6.3.6.1. Survivability Overview

6.3.6.2. Survivability Parameters/Requirements

6.3.6.3. Survivability Planning

6.3.6.1. Survivability Overview

Survivability factors consist of those system design features that reduce the risk of fratricide, detection, and the probability of being attacked; and that enable the crew to withstand man-made hostile environments without aborting the mission or suffering acute chronic illness, disability, or death. Survivability attributes, as described in the Joint Military Dictionary (JP 1-02), are those that contribute to the survivability of manned systems. In the HSI construct, the human is considered integral to the system and personnel survivability should be considered in the encompassing "system" context.

6.3.6.2. Survivability Parameters/Requirements

A Survivability / Force Protection Key Performance Parameter should be considered for any "manned system or system designed to enhance personnel survivability" when the system may be employed in an asymmetric threat environment. The Capability Development Document should include applicable survivability parameters. This may include requirements to eliminate significant risks of fratricide or detectability, or to be survivable in a nuclear, biological, and chemical (NBC) battlefield. NBC survivability, by definition, includes the instantaneous, cumulative, and residual effects of NBC weapons upon the system, including its personnel. It may be appropriate to require that the system "permit performance of mission-essential operations, communications, maintenance, re-supply and decontamination tasks by suitably clothed, trained, and acclimatized personnel for the survival periods and NBC environments required by the system."

The consideration of survivability should also include system requirements to ensure the integrity of the crew compartment and rapid egress when the system is damaged or destroyed. It may be appropriate to require that the system provide for adequate emergency systems for contingency management, escape, survival, and rescue.

6.3.6.3. Survivability Planning

The Joint Capabilities Integration and Development System capability documents define the program's combat performance and survivability needs. Consistent with those needs, the program manager should establish a survivability program. This program, overseen by the program manager, should seek to minimize (1) the probability of encountering combat threats, (2) the severity of potential wounds and injury incurred by personnel operating or maintaining the system, and (3) the risk of potential fratricidal incidents. To maximize effectiveness, the program manager should assess survivability in close coordination with systems engineering and test and evaluation activities.

Survivability assessments assume the warfighter is integral to the system during combat. Damage to the equipment by enemy action, fratricide, or an improperly functioning component of the system can endanger the warfighter. The survivability program should assess these events and their consequences. Once these initial determinations are made, the design of the equipment should be evaluated to determine if there are potential secondary effects on the personnel. Each management decision to accept a potential risk should be formally documented by the appropriate management level as defined in DoD Instruction 5000.02.

During early stages of the acquisition process, sufficient information may not always be available to develop a complete list of survivability issues. An initial report is prepared listing those identified issues and any findings and conclusions. Classified data and findings are to be appropriately handled according to each DoD Component's guidelines. Survivability issues typically are divided into the following components:

- **Reduce Fratricide.** Fratricide is the unforeseen and unintentional death or injury of "friendly" personnel resulting from friendly forces employment of weapons and munitions. To avoid these types of survivability issues, personnel systems and weapon systems should include anti-fratricide systems, such as Identification of Friend or Foe and Situational Awareness systems.
- **Reduce Detectability.** Reduce detectability considers a number of issues to minimize signatures and reduce the ranges of detection of friendly personnel and equipment by confounding visual, acoustic, electromagnetic, infrared/thermal, and radar signatures and methods that may be utilized by enemy equipment and personnel. Methods of reducing detectability could include camouflage, low-observable technology, smoke, countermeasures, signature distortion, training, and/or doctrine.
- **Reduce Probability of Attack.** Analysts should seek to reduce the probability of attack by avoiding appearing as a high value-target and by actively preventing or deterring attack by warning sensors and use of active countermeasures.
- **Minimize Damage if Attacked.** Analysts should seek to minimize damage, if attacked, by: 1) designing the system to protect the operators and crewmembers from enemy attacks; 2) improving tactics in the field so survivability is increased; 3) designing the system to protect the crew from on-board hazards in the event of an attack (e.g., fuel, munitions, etc.); and, 4) designing the system to minimize the risk to supporting personnel if the system is attacked. Subject matter experts in areas such as nuclear, biological and chemical warfare, ballistics, electronic warfare, directed energy, laser hardening, medical treatment, physiology, human factors, and Information Operations can add additional issues.
- **Minimize Injury.** Analysts should seek to minimize: 1) combat, enemy weapon-caused injuries; 2) the combat-damaged system's potential sources and types of injury to both its crew and supported troops as it is used and maintained in the field; 3) the system's ability to prevent further injury to the fighter after being attacked; and 4) the system's ability to support treatment and evacuation of injured personnel. Combat-caused injuries or other possible injuries are addressed in this portion of personnel survivability, along with the different perspectives on potential mechanisms for reducing damage. Evacuation capability and personal equipment needs (e.g. uniform straps to pull a crew member through a small evacuation port are addressed here.
- **Minimize Physical and Mental Fatigue.** Analysts should seek to minimize injuries that can be directly traced to physical or mental fatigue. These types of injuries can be traced to complex or repetitive tasks, physically taxing operations, sleep deprivation, or high stress environments.
- **Survive Extreme Environments.** This component addresses issues that will arise once the warfighter evacuates or is forced from a combat-affected system such as an aircraft or watercraft and must immediately survive extreme conditions encountered in the sea or air until rescued or an improved situation on land is reached. Dependent upon requirements, this may also include some extreme environmental conditions found on land, but generally this component is for sea and air where the need is immediate for special consideration to maintain an individual's life. Survival issues for downed pilots behind enemy lines should be considered here.

The program manager should summarize plans for survivability in the Life-Cycle Sustainment Plan and address survivability risks and plans for risk mitigation. If the system or program has been designated by Director, Operational Test & Evaluation, for live fire test and evaluation (LFT&E) oversight, the program manager should integrate T&E to address crew survivability issues into the LFT&E program to support the Secretary of Defense LFT&E Report to Congress (10 USC 2366). The program manager should address special equipment or gear needed to sustain crew operations in the operational environment.

6.3.7. Habitability

6.3.7.1. Habitability Overview

Habitability factors are those living and working conditions that are necessary to sustain the morale, safety, health, and comfort of the user population. They directly contribute to personnel effectiveness and mission accomplishment, and often preclude recruitment and retention problems. Examples include: lighting, space, ventilation, and sanitation; noise and temperature control (i.e., heating and air conditioning); religious, medical, and food services availability; and berthing, bathing, and personal hygiene

Habitability consists of those characteristics of systems, facilities (temporary and permanent), and services necessary to satisfy personnel needs. Habitability factors are those living and working conditions that result in levels of personnel morale, safety, health, and comfort adequate to sustain maximum personnel effectiveness, support mission performance, and avoid personnel retention problems.

6.3.7.2. Habitability Parameters/Requirements

Habitability is one of several important factors included in the overall consideration of unit mission readiness. Per DoD Instruction 5000.02, the program manager shall work with habitability representatives to establish requirements for the physical environment (e.g., adequate light, space, ventilation, and sanitation, and temperature and noise control) and, if appropriate, requirements for personal services (e.g., religious, medical, and mess) and living conditions (e.g., berthing and personal hygiene) if the habitability factors have a direct impact on meeting or sustaining performance requirements, sustaining mission effectiveness, or that have such an adverse impact on quality of life or morale that recruitment or retention rates could be degraded. Examples include requirements for heating and air-conditioning, noise filters, lavatories, showers, dry-cleaning and laundry.

While a system, facility, and/or service should not be designed solely around optimum habitability factors, habitability factors cannot be systematically traded-off in support of other readiness elements without eventually degrading mission performance.

6.3.7.3. Habitability Planning

The program manager should address habitability planning in the Life-Cycle Sustainment Plan and identify habitability issues that could impact personnel morale, safety health, or comfort or degrade personnel performance, unit readiness, or result in recruitment or retention problems.

6.4. Human Systems Integration (HSI) throughout the System Life Cycle

6.4.1. Research and Development (R&D), Studies, and Analyses in Support of Human Systems Integration (HSI)

Continuous application of human-centered research data, methods, and tools will ensure maximum operational and training effectiveness of the system. Continual analysis of system functionality provides data to help determine the best allocation of tasks to personnel, hardware, or software. Results guide human workload predictions, man-machine interface requirements,

and procedural, software, and hardware innovations needed to ensure that the human element can fulfill and enhance total system performance. Each military department conducts human centered research. The products of this research form the basis for creating and maintaining military standards, design criteria, methodologies, tools, and data bases used when applying HSI to defense systems acquisition. Within each military department, HSI practitioners support ongoing concepts and studies that identify potential HSI impacts on operational effectiveness and resource needs of alternative solutions. Examples of these activities include field assessments, human performance modeling, simulations, and technology demonstrations.

It is equally important that this research work be rolled into the front end analyses that lead to capability requirements. HSI considerations should be carefully examined during the capabilities-based assessment, and the planning for and execution of the Analyses of Alternatives. Failure to examine the human-centric issues up front may unduly complicate integration in a defined materiel solution.

6.4.2. Human Systems Integration (HSI) in the Capabilities Documents

The Initial Capabilities Document may seek to establish a new capability, improve an existing capability, or exploit an opportunity to reduce costs or enhance performance. The Initial Capabilities Document shall describe the key boundary conditions and operational environments that impact how the system is employed to satisfy the mission need. Key boundary conditions include critical manpower, personnel, training, environment, safety, occupational health, human factors, habitability, and survivability factors that have a major impact on system performance and life-cycle costs. The Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, or Facilities considerations and implications section of the Initial Capabilities Document should discuss all relevant domains of HSI.

HSI capabilities in the Capability Development Document should be specified in measurable, testable, performance-based language that is specific to the system and mission performance. Analyses and results conducted to determine the HSI requirements should be identified in and governed by other programmatic documentation (e.g., HSI plan, Systems Engineering Plan, Training Systems plan, or Manpower Estimate).

6.4.2.1. Refining Required Capabilities

As plans for the system mature, the capabilities documents should become more specific and reflect the integration of program objectives. The program manager should work with Human Systems Integration (HSI) practitioners and user representatives to translate HSI thresholds and objectives in the capabilities documents into quantifiable and measurable system requirements. The program manager should refine and integrate operational and design requirements so they result in the proper balance between performance and cost, and keep programs affordable. Additionally, system requirements should serve as the basis for developing engineering

specifications, and should be reflected in the statement of work, contracts, Test and Evaluation Master Plan, and other program documentation. Over the course of the acquisition process, as trade-offs are made and plans for the system design mature, the capabilities documents should be updated to reflect a more refined and integrated set of parameters.

6.4.3. Engineering and Manufacturing Development Phase

The purpose of the Engineering and Manufacturing Development phase is to develop a system or an increment of capability; reduce integration and manufacturing risk (technology risk reduction occurs during Technology Development); ensure operational supportability with particular attention to reducing the logistic footprint; implement Human Systems Integration; design for producibility; ensure affordability and protection of critical program information by implementing appropriate techniques such as anti-tamper; and demonstrate system integration, interoperability, safety and utility.

6.4.3.1. Solicitations and Source Selection

Human Systems Integration considerations should be clearly defined and given proper weight in solicitations and proposal evaluation guidelines provided to the government evaluation team. The record of contractors in safety and implementation of human engineering can be an element of bid selection and contract performance criteria.

6.4.3.2. Systems Engineering

Once parameters are established in the Initial Capabilities Document and Capability Development Document, it is the program manager's responsibility to ensure that they are addressed during the systems engineering process, included in the Human Systems Integration (HSI) Plan and the Systems Engineering Plan (SEP), and properly considered during cost/performance trade-off analyses. Consistent with paragraph E1.1.29 of DoD Directive 5000.01, the program manager shall apply HSI to optimize total system performance, operational effectiveness, suitability, survivability, safety, and affordability. Program managers shall consider supportability, life-cycle costs, performance, and schedule comparable in making program decisions. Each program is required to have a comprehensive plan for HSI. It is important that this plan be included in the SEP or as a stand alone HSI Plan as the program(s) may require. As required by DoD Instruction 5000.02, the program manager shall take steps (e.g., contract deliverables and Government/contractor Integrated Product Teams) to ensure human factors engineering/cognitive engineering is employed during systems engineering from Materiel Solution Analysis phase through the life of the program to provide for effective human-machine interfaces, meet HSI requirements, and (as appropriate) support a system-of-systems acquisition approach. The program manager should also ensure that HSI requirements are included in performance specifications and test criteria. Manpower, Personnel, and Training functional representatives, as user representatives, participate in the systems engineering process to help produce the proper balance between system performance and cost and to ensure that

requirements remain at affordable levels. Manpower, personnel, training, and supportability analyses should be conducted as an integral part of the systems engineering process throughout the acquisition life cycle, beginning with Materiel Solution Analysis and continuing throughout program development.

6.4.3.2.1. System Design

Human Systems Integration (HSI) plays a major role in the design process. Front-end analysis methods, such as those described in MIL-HDBK-46855A, should be pursued to maximize the effectiveness of the new system. Initial emphasis should be placed on "lessons learned" from legacy, predecessor or comparable systems to help identify and eliminate characteristics in the new system that require excessive cognitive, physical, or sensory skills or high aptitudes; involve complex fault location or workload intensive tasks; necessitate excessive training; require proficiency training; or result in frequent or critical errors or safety/health hazards. Placing an emphasis on the "human-in-the-loop" ensures that systems are designed to operate consistent with human performance capabilities and limitations, meet system functional requirements, and fulfill mission goals with the least possible demands on manpower, personnel, and training. Moreover, sound HSI applications can minimize added costs that result when systems have to be modified after they are fielded in order to correct performance and safety issues.

6.4.3.2.2. Allocations

During systems engineering, analyses should be performed iteratively to define successively lower functional and performance requirements, to identify functional interfaces, and to allocate functions to components of the system (e.g., hardware, software, and human). Tasks should be allocated to the human component consistent with human attributes (i.e., capabilities and limitations) of the user population as established in the Target Audience Description. Requirements analysis should be conducted iteratively in conjunction with logical analysis to develop and refine system level performance requirements, identify external interfaces, and provide traceability among user requirements and design requirements. Human-machine interfaces should be identified as an outgrowth of the functional allocation process. Another product of the systems engineering process is a list of job tasks with performance/confidence levels. This information is used to further refine manpower, personnel and training requirements.

6.4.3.2.3. Specifications and Standards

It is primarily the responsibility of the program manager, with the assistance of the Integrated Product Teams, to establish performance specifications, design criteria standards, interface standards, and data specifications in the solicitation and resulting contract. Strong consideration should be given to establishing standards when uniform configuration is necessary for ease of operation, safety, or training purposes. For instance, a control panel or avionics suite may need to be standardized to enhance the ability of the user to access information and to respond quickly in an emergency situation. Standard features preclude the need to teach multiple (or conflicting)

responses to similar tasks. Standardization is particularly important when a standard performance is required for safety reasons. For instance, rapid ejection from the cockpit should require standard procedures and tasks. If there are unique health hazard or survivability requirements, such as vibration or shock tolerances, extended temperature range, or noise levels, standardization may be the most efficient way to ensure that the system meets those special requirements. Preference should be given to specifications and standards developed under the Defense Standardization Program. Regulatory occupational exposure standards create performance thresholds. However, use of guidance exposure criteria and ergonomic/Human Systems Integration guidelines should be considered to ensure personnel protection, promote efficiency, and anticipate more stringent standards that are likely to be required during the life cycle of the system.

Performance standards for operators, maintainers, both individual and team, are derived from the performance requirements of the total system. For example, human performance requirements (e.g., completion times or success rates) presumes that in order for the total system to achieve specified performance levels, the human will have to complete tasks or achieve performance objectives within specified confidence levels (usually expressed in terms of per cent of actions completed within a specified time-frame and/or error limit). The training/instructional system should be developed to ensure that operators can meet or exceed the personnel performance levels required to operate/maintain the systems. Additionally, manpower should be determined based on these same performance requirements. Operational tests should also be based on the same criteria.

6.4.4. Production and Deployment

The objective of this phase of the acquisition process is to achieve an operational capability that satisfies mission needs. Operational test and evaluation shall determine the effectiveness and suitability of the system.

6.4.5. Operations and Support (O&S)

The objective of this phase is the execution of a support program that meets operational support performance requirements and sustains the system in the most cost-effective manner over its life cycle. As required by DoD Directive 5000.01, planning for O&S shall begin as early as possible in the acquisition process. Efforts during the O&S phase should be directed towards ensuring that the program meets and has the resources to sustain the threshold values of all support performance requirements. Once the system is fielded or deployed, a follow-on operational testing program, to assess performance, quality, compatibility, and interoperability, and identify deficiencies, should be conducted, as appropriate. Post fielding verification of the manpower, and information resulting from training exercises, readiness reports, and audits can also be used to assess the operational capability of the system. During fielding, deployment, and throughout operational support, the need for modifications to the system should be assessed.

6.5. Affordability

6.5. Affordability

Consistent with DoD Directive 5000.01, all participants in the acquisition system shall recognize the reality of fiscal constraints. The user shall address affordability when establishing capability needs and at each milestone decision point. As required by DoD Instruction 5000.02:

> *An affordability determination results from the process of addressing cost during the requirements process and is included in each CDD using life-cycle cost or, if available, total ownership cost. Transition into EMD also requires full funding (i.e., inclusion of the dollars and manpower needed for all current and future efforts to carry out the acquisition strategy in the budget and out-year program), which shall be programmed in anticipation of the Milestone B decision. . . . In no case shall Milestone B be approved without full funding. . . .*

6.5.1. Life-cycle Cost Objectives

As required by DoD Directive 5000.01, the estimation of ownership costs shall begin as early as possible in the acquisition process. Life-cycle cost objectives are usually established prior to program initiation. These objectives embody the planned affordability for the program. At each subsequent milestone review, the Milestone Decision Authority assesses life-cycle cost objectives and progress towards achieving them.

The operating and support portion of the life-cycle costs should be consistent with manpower, personnel, and training constraints established in the Capability Development Document.

6.5.2. Manpower Estimates

Manpower Estimate shall address manpower affordability in terms of military end strength (including force structure and student end strength) and civilian work years beginning at Milestone B. Additionally, the use of contractor workyears support should also be documented, where possible. Consistent with DoD Directive 5000.01, DoD Components shall plan programs based on realistic projections of the dollars and manpower likely to be available in future years. When major manpower increases are required to support the program, or major manpower shortfalls exist, they shall be identified as risks in the Manpower Estimate, and addressed in the risk assessment section of the Acquisition Strategy. Program risks that result from manpower

shortfalls should be addressed in terms of their impact on readiness, operational availability, or reduced combat capability.

6.5.3. Cost as an Independent Variable

DoD Directive 5000.01 requires the program manager to view cost as an independent variable. During trade-off analysis, program managers should consider whether it is more cost effective for the Department to spend additional money during the engineering and design process to achieve a system with reduced support costs than it is to design a more resource intensive system at reduced acquisition costs. Such comparisons should consider all aspects of life-cycle costs, including mishaps resulting in lost work time.

6.6. Additional References

6.6.1. DoD Publications

The following DoD Directives and Instructions provide policy and direction:

- DoD Directive 1100.4, "Guidance for Manpower Programs"
- DoD Directive 1322.18, "Military Training"
- DoD Instruction 1100.22, "Guidance for Determining Workforce Mix"
- DoD Instruction 1322.20, "Development and Management of Interactive Courseware for Military Training"
- Training Transformation Implementation Plan
- CJCS Instruction 3170.01, "Joint Capabilities Integration and Development System"
- The JCIDS Manual, "Operation of the Joint Capabilities Integration and Development System"
- Joint Military Dictionary (JP 1-02), "Department of Defense Dictionary of Military and Associated Terms"
- AR 602-2, "Manpower and Personnel Integration (MANPRINT) in the Systems Acquisition Process"

6.6.2. Discretionary Practices

The following military standards (MIL-STD), DoD Handbooks (DOD-HDBK), and Military handbooks (MIL-HDBK) can be used to support Human Systems Integration analysis:

- MIL-STD-882D, "Standard Practice for System Safety"

- MIL-STD-1472, "DoD Design Criteria Standard: Human Engineering"
- DOD-HDBK-743, "Anthropometry of U. S. Military Personnel"
- MIL-HDBK-759, "Human Engineering Design Guidelines"
- MIL-HDBK-46855A, "Human Engineering Program Process and Procedures"
- MIL-PRF-29612, "Performance Specification, Training Data Products"
- "A Guide for Early Embedded Training Decisions," U.S. Army Research Institute for the Behavioral and Social Sciences Research Product 96-06.

DEFENSE ACQUISITION GUIDEBOOK
Chapter 7 -- Acquiring Information Technology, Including National Security Systems

7.0. Overview

7.0.1. Purpose

The goal of this chapter is to help program managers (PMs) and Sponsors/Domain Owners implement Department of Defense (DoD) policies intended to achieve "fundamentally joint, net-centric, distributed forces capable of rapid decision superiority and massed effects across the battle space." This chapter explains how the DoD is using a net-centric strategy to transform DoD warfighting, business, and intelligence capabilities. The chapter provides descriptions and explanations of many of the associated topics and concepts. This chapter also discusses many of the activities that enable the development of net-centric systems, however, not all activities are the direct responsibility of the PM. Many activities reflect Department-level effort that occurs prior to or outside of the acquisition process. The detailed discussions of such a broad set of

activities are presented here to help the PM understand the context of the capabilities described in the Joint Capabilities Integration and Development System (JCIDS) documents and required of the system under development.

7.0.2. Contents

This chapter contains ten sections that present the Program Manager with a comprehensive review of topics, concepts, and activities associated with the acquisition of Information Technology (IT), including National Security Systems (NSS).

Section 7.1, "Introduction," explains net-centric information sharing in the context of the discussions and requirements outlined in the various other sections of this chapter.

Section 7.2, "DoD Information Enterprise (DoD IE)," explains several important concepts that provide a foundation for acquiring net-centric Information Technology (including NSS). The overarching concept is that the DoD Enterprise Architecture (DoD EA) is used to describe and document current and desired relationships among warfighting operations, business, and management processes, the entities involved, and the information used. The IT architectures (i.e., IT solutions) are then aligned with the DoD EA.

DoDAF views that comprise architectures that are the DoD EA, and the DoD EA as a whole:

- Describe existing and desired capabilities.
- Provide a basis for interoperability and supportability reviews and certifications.
- Provide a component of the Net-Ready Key Performance Parameter.
- Provide required components of the Capability Development Document (CDD) and Capability Production Document (CPD).

The section discusses the DoD IEA V1.1 and its role in helping PMs and Sponsors/Domain Owners describe their transition from the current environment to the future net-centric environment. Sections 7.3 through 7.10 elaborate on specific areas on which the Sponsors/Domain Owners and PMs should focus as they work to deliver and improve the reach, richness, agility, and assurance of net-centric capabilities.

Section 7.3, "Interoperability and Supportability of Information Technology and National Security Systems," explains interoperability and supportability, outlines the use of the Net-Ready Key Performance Parameter in these processes, and describes the process of building an Information Support Plan.

Section 7.4, "Net-centric Information Sharing Data Strategy," provides guidance on implementing the Net-centric Data Strategy and outlines important data tasks as they relate to the acquisition process.

Section 7.5, "Information Assurance," explains the requirements for Information Assurance and provides links to resources to assist in developing an Information Assurance strategy.

Section 7.6, "Electromagnetic Spectrum," offers a discussion and explanation of Spectrum Supportability.

Section 7.7, "Accessibility of Electronic and Information Technology," summarizes the requirements of the Workforce Investment Act of 1998, (Section 508 of the Rehabilitation Act (as amended in 1998)), regarding the procurement, development, maintenance, or use of electronics and IT that are accessible to people with disabilities.

Section 7.8, "Clinger-Cohen Act," helps PMs and Sponsors/Domain Owners understand how to implement Subtitle III of title 40 United States Code (formerly know as division E of the Clinger-Cohen Act (CCA) and hereinafter referred to as "Title 40/CCA") and associated regulatory requirements.

Section 7.9, "Post Deployment Reviews," discusses how the Department of Defense (DoD) uses the Post Implementation Review to inform Sponsors of the degree to which their IT/NSS investments closed the needed capability gaps.

Section 7.10, "Commercial, Off-The-Shelf (COTS) Solutions," provides insight into DoD guidance regarding acquisition of COTS software products.

In summary, this chapter should help PMs and Sponsors/Domain Owners understand and apply the tools of the DoD EA so that they can more effectively:

- Describe and measure the degree to which their programs are interoperable and supportable with the DoD IE.
- Ensure their programs employ and institutionalize approaches that make data visible, accessible, understandable, trusted, interoperable and responsive.
- Achieve the Department's objectives for Information Assurance.
- Ensure their programs will have assured interoperable access to electromagnetic spectrum.
- Achieve these goals within the constraints of the law and where possible, through the use of commercially available solutions.

7.1. Introduction

The DoD Transformation Planning Guidance (April 2003) defines the desired outcome of transformation as "fundamentally joint, network-centric, distributed forces capable of rapid decision superiority and massed effects across the battle space." The goal of this chapter is to help Program Managers and Sponsors/Domain Owners implement the DoD policies that are intended to achieve this outcome. This introduction briefly explains net-centricity in context of the requirements outlined in the various other sections of this chapter.

Net-centric information sharing is "the realization of a robust, globally networked environment (interconnecting infrastructure, systems, processes, and people) within which data is shared seamlessly and in a timely manner among users, applications, and platforms. By securely interconnecting people and systems, independent of time or location, net-centricity enables substantially improved military situational awareness and significantly shortened decision making cycles. Users are empowered to better protect assets; more effectively exploit information; more efficiently use resources; and unify our forces by supporting extended, collaborative communities to focus on the mission."

The Department's approach for transforming to net-centric operations and warfare and achieving the net-centric information sharing vision focuses on five, key areas where increased attention and investment will bring the most immediate progress towards realizing net-centric goals:

- Data and Services
- Secured Availability
- Computing Infrastructure Readiness
- Communications Readiness
- NetOps Agility

This approach uses the Information Enterprise (IE) as "the organizing and transforming construct for managing information technology throughout the Department." It envisions moving to trusted network-centric operations through the acquisition of services and systems that are secure, reliable, interoperable, and able to communicate across a universal Information Technology infrastructure, to include National Security Systems. This Information Technology infrastructure includes data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities. The rest of this chapter describes the concepts, topics, and activities to achieve this transformation.

7.2. DoD Information Enterprise

7.2.1. Introduction

7.2.1. Introduction

To provide a conceptual framework for this change, the Department has defined a Department of Defense Information Enterprise (DoD IE) as an organizing construct. The DoD IE consists of the Department of Defense information assets, processes, activities, and resources required to achieve an information advantage and share information across the Department and with mission partners. The DoD IE includes:

- The information itself, which is a key asset to the Department, and the Department's management over the information life cycle.
- The processes, including risk management, associated with managing information to accomplish the DoD mission and functions.
- Activities related to designing, building, populating, acquiring, managing, operating, protecting and defending the information enterprise.
- Related information resources such as personnel, funds, equipment, and information technology, including national security systems.

7.2.1.1. Information Enterprise Vision

The Department of Defense Information Enterprise (DoD IE) vision is transforming the Department into an agile enterprise empowered by access to and sharing of timely and trusted information. The net-centric vision of the DoD IE is to function as one unified DoD Enterprise, creating an information advantage for our people and mission partners by providing:

- A rich information sharing environment in which data and services are visible, accessible, understandable, and trusted across the enterprise.
- An available and protected network infrastructure (the Global Information Grid (GIG)) that enables responsive information-centric operations using dynamic and interoperable communications and computing capabilities.

Program Managers and Sponsors/Domain Owners should use this vision to help guide their acquisition programs. This vision requires a comprehensive information capability that is global, robust, survivable, maintainable, interoperable, secure, reliable, and user-driven to be operationally suitable, safe, effective, usable and affordable across the life cycle of the systems.

7.2.1.2. The Information Technology (IT) Infrastructure of the Department

The IT infrastructure of the Department is the Global Information Grid (GIG). The GIG is the Department's globally interconnected end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. Non-GIG IT includes stand-alone, self-contained, or embedded IT that is not and will not be connected to the enterprise network.

Every DoD acquisition program having an IT component is a participant in the GIG. Each new IT-related acquisition program replaces, evolves, or adds new capabilities to the GIG. Components, Combat Developers, Sponsors, Domain Owners, DoD Agencies, and PMs should consider the existing and planned capabilities of the GIG that might be relevant as they develop their integrated architectures, Joint Capabilities Integration and Development System documentation (see the JCIDS Manual), and related program requirements.

7.2.1.3. The DoD Enterprise Architecture

An Enterprise Architecture describes the "current architecture" and "target architecture," and provides a strategy that will enable an agency to transition from its current state to its target environment. The Office of Management and Budget defines enterprise architecture as the explicit description and documentation of the current and desired relationships among business and management processes and IT. All DoD architectures, including warfighter, intelligence, business process, and enterprise management architectures, are part of the DoD EA. The DoD EA is defined as a federation of descriptions that provide context and rules for accomplishing the mission of the Department. These descriptions are developed and maintained at the Department, Capability Area, and Component levels and collectively define the people, processes, and technology required in the "current" and "target" environments, and the roadmap for transition to the target environment. As the Secretary of Defense's principal staff assistant for IT and information resources management, the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) develops, maintains, and facilitates the use of the DoD EA to guide and oversee the evolution of the Department's IT-related investments to meet operational needs.

7.2.1.4. DoD Information Enterprise Architecture

The DoD Information Enterprise Architecture (IEA) V1.1 provides a common foundation to support accelerated DoD transformation to net-centric operations and establishes priorities to address critical barriers to its realization.

The published DoD IEA V1.1 describes the integrated Defense Information Enterprise and the rules for the information assets and resources that enable it. DoD IEA V1.1 unifies the concepts embedded in the Department's net-centric strategies into a common vision, providing relevance and context to existing policy. DoD IEA V1.1 highlights the key principles, rules, constraints and

best practices drawn from collective policy to which applicable DoD programs, regardless of Component or portfolio, must adhere in order to enable agile, collaborative net-centric operations. In today's information environment the DoD IEA V1.1 rules apply within the persistently-connected Internet Protocol boundaries of the GIG. Outside of these boundaries, the principles still should be considered, but the rules of the DOD IEA V1.1 must yield to the state of technology, and the needs and imperatives of the Department's missions.

7.2.2. Mandatory Policies

7.2.2.1. DoD Directive 5000.01, "The Defense Acquisition System"

Extracts:

- *E1.1.9: Information Assurance. Acquisition managers shall address information assurance requirements for all weapon systems; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems; and information technology programs that depend on external information sources or provide information to other DoD systems.*
- *E1.1.10: Information Superiority. Acquisition managers shall provide U.S. Forces with systems and families of systems that are secure, reliable, interoperable, compatible with the electromagnetic spectrum environment, and able to communicate across a universal information technology infrastructure, including NSS, consisting of data, information, processes, organizational interactions, skills, analytical expertise, other systems, networks, and information exchange capabilities.*
- *E1.1.13: Interoperability. Systems, units, and forces shall be able to provide and accept data, information, materiel, and services to and from other systems, units, and forces and shall effectively interoperate with other U.S. Forces and coalition partners. Joint concepts and integrated [solution] architectures shall be used to characterize these interrelationships.*

7.2.2.2. DoD Instruction 5000.02, "Operation of the Defense Acquisition System"

Extract:

- *The DoD Enterprise Architecture shall underpin all information architecture development. In accordance with DoD Directive 8000.01 . . ., each integrated solution architecture shall have three views: operational, systems, and technical. The standards used to form the technical views of integrated architectures shall be selected from those contained in the current approved version of the DoD IT Standards Registry.*

DoD Instruction 5000.02 requires DoD acquisition programs to demonstrate consistency with GIG policies and architectures, to include relevant standards. (See Enclosure 5, Table 8, Title 40, Subtitle III/CCA Compliance Table) (The table indicates that the Net-Ready Key Performance Parameter in the Acquisition Program Baseline, required at Program Initiation for Ships, Milestone (MS) B, MS C, and the Full-Rate Production Decision Review (DR) (or Full Deployment DR), in part satisfies the requirement. The table also indicates that the Information Support Plan (ISP), in part, satisfies the requirement. An Initial ISP is required at Program Initiation for Ships and at MS B. A Revised ISP is due at the Critical Design Review (unless waived). And the ISP of Record is due at MS C.)

The DoD components under ASD(NII)/DoD CIO leadership are required to develop and implement the Federated DoD Enterprise Architecture and transition plans for acquiring Information Technology (IT) (including National Security Systems) and to use them to guide the acquisition of IT.

Each IT acquisition program (or set of programs) is also required to develop an integrated solution architecture and implementation plan per the DoD Architecture Framework (DoDAF) and use these products over the program life cycle to guide, monitor, and implement solutions in alignment with the Federated DoD Enterprise Architecture.

Using these architectures and plans, the ASD(NII)/DoD CIO, in collaboration with Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) and portfolio managers will conduct capability assessments, guide systems development, and define the associated investment plans as the basis for aligning resources throughout the Planning, Programming, Budgeting, and Execution process.

7.2.2.3. CJCS Instruction 6212.01, "Interoperability and Supportability of Information Technology (IT) and National Security Systems"

It is DoD policy that all Information Technology (IT) and National Security Systems (NSS) and major modifications to existing IT and NSS will be compliant with the Title 40/CCA, DoD

interoperability regulations and policies, and the most current version of the DoD Information Technology Standards Registry (DISR). Establishing interoperability and supportability in a DoD system is a continuous process that must be managed throughout the life cycle of the system. The following elements comprise the Net-Ready Key Performance Parameter (NR-KPP): 1) compliant integrated architecture; 2) compliance with DoD Net-centric Data and Services strategies; 3) compliance with applicable GIG Technical Guidance; 4) verification of compliance with DoD information assurance requirements; and 5) compliance with supportability elements to include spectrum utilization and information bandwidth requirements, Selective Availability Anti-Spoofing Module (SAASM) and the Joint Tactical Radio System, as applicable. (See CJCSI 6212.01, Enclosure A, paragraph 1.e.)

7.2.2.4. DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"

This Directive defines a capability-focused, effects-based approach to advance IT and NSS interoperability and supportability across the Department of Defense.

Extract:

- *1.3. Establishes the Net-Ready Key Performance Parameter (NR-KPP) to assess net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP replaces the Interoperability KPP and incorporates net-centric concepts for achieving IT and NSS interoperability and supportability.*
- *4.2. IT and NSS, of the DoD Global Information Grid (GIG), shall provide for easy access to information, anytime and anyplace, with attendant information assurance. The GIG architecture shall be used as the organizing construct for achieving net-centric operations and warfare.*

7.2.2.5. DoD Directive 8000.01, "Management of the DoD Information Enterprise"

This document reissues and renames DoD Directives 8000.01 and cancels 8100.01. The new DoD Directive 8000.01 requires the following:

- All aspects of the Defense Information Enterprise, including the Global Information Grid (GIG) infrastructure and enterprise services and solutions be planned, designed, developed, configured, acquired, managed, operated, and protected to achieve a net-centric environment, as envisioned in the National Defense Strategy, and be capable of effectively and efficiently supporting the Department's outcome goals and priorities.
- Investments in information solutions be managed through a capital planning and investment control process that is performance- and results-based; and provides for

analyzing, selecting, controlling, and evaluating investments, as well as assessing and managing associated risks.

- The capital planning and investment control process interface with the DoD key decision support systems for capability identification; planning, programming, budgeting, and execution; and acquisition.
- Review of all Information Technology (IT) investments for compliance with architectures, IT standards, and related policy requirements.
- Acquisition strategies appropriately allocate risk between the Government and contractor; effectively use competition; tie contract payments to performance; and, where practicable, take maximum advantage of commercial off-the-shelf and non-developmental item technology.
- Information solutions structured in useful segments, narrow in scope and brief in duration; each segment solves a specific part of the overall mission problem and delivers a measurable net benefit independent of future segments.

DoD Directive 8000.01 encourages pilots, modeling and simulation, experimentation, and prototype projects, appropriately sized to achieve desired objectives, and not be used in lieu of testing or acquisition processes to implement the production version of the information solution.

7.2.3. The Use of Architecture

7.2.3.1. Compliance with the DoD Information Enterprise (DoD IE)

7.2.3.2. Compliance with the DoD Information Enterprise Architecture (IEA)

7.2.3.3. Net-Centric Attributes

7.2.3.4. Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))/DoD Chief Information Officer (CIO) Use of the DoD IEA

7.2.3. The Use of Architecture

a. Architectures are tools to improve the operational processes, infrastructure, and materiel solutions of the Department. Architecture-enabled solutions should facilitate improved interoperability, better information sharing, tighter compliance, leaner processes, reduced costs, and more effective mission accomplishment.
b. The DoD Enterprise Architecture (EA), comprised of the DoD enterprise and DoD Component level architectures, should guide investment portfolio strategies and decisions, define capability and interoperability requirements, establish and enforce standards, guide security and information assurance requirements across the Department of Defense, and provide a sound basis for transition from the existing environment to the future. Solutions should conform to the DoD EA.
c. Solution architectures should be developed for material and non-material initiatives and capabilities that deliver functionality for the DoD information enterprise.

d. All information technology investments, including those related to National Security Systems, should be reviewed for compliance with the DoD Enterprise Architecture and applicable approved solution architectures, and alignment with the Federal Enterprise Architecture (FEA).
e. An architecture is considered a strategic information asset and should be appropriately secured, shared and made available to any DoD user or mission partner to the maximum extent allowed by law and DoD policy.

7.2.3.1. Compliance with the DoD Information Enterprise (DoD IE)

To comply with the DoD IE, an information technology (IT)-based initiative or an acquisition program, throughout its life cycle should:

- Meet the DoD Architecture Framework (DoDAF) requirements in producing architectural views. This requirement is met by producing a complete integrated architecture using the specified models and vocabulary described in the DoDAF and having it assessed for accuracy, consistency, and sufficiency with respect to its intended use (e.g., capability definition, process re-engineering, investment decisions, and integration engineering).
- Meet the DODAF Meta-model (DM2) Physical Exchange Specification (PES) requirements for sharing/reusing architecture data. This requirement is met through the program's creation of XML, based on the PES XSD for the necessary and foundational DM2 concepts and through contributing new reusable architecture data (if any) to the DM2.
- Meet the DoD Information Technology (IT) Standards Registry (DISR) requirements in selecting technologies and standards. This requirement is met by defining and implementing capabilities, based on technologies and standards contained within the Joint Technical Architecture (JTA)/DISR. Meeting this requirement should be validated at every milestone. When building systems, requests for proposals and contract statements of work should be reviewed as part of approved acquisition processes to ensure IT standards established in Initial Capabilities Documents, Capability Development Documents, and Capability Production Documents are translated into clear contractual requirements. In addition, requests for proposals and contract statements of work should contain additional requirements for contractors to identify instances where cost, schedule, or performance impacts may preclude the use of IT standards mandated in DISR.
- Meet the DoD Net-Centric Data Strategy requirements and intent. Make explicit the data that is produced and used by the program's implemented operations. Provide the associated metadata, and define and document the program's data models. This requirement is met by:
    - Describing the metadata that has been registered in the DoD Data Metadata Registry for each data asset used and for each data asset produced (i.e., data for which the program is the Source Data Authority).
    - Providing the documented data models associated with the program.

- Explicitly address net-centric information sharing and determining the program's net-centric correspondence to key net-centric criteria (e.g., concepts, processes, services, technologies, standards, and taxonomy). (For further information see the DoD Information Enterprise Architecture (IEA) V1.1.)
- Meet the broad requirements set forth in the Global Information Grid (GIG) Capstone Requirements Document. This requirement is met by describing the program elements that address each requirement and by expressing an overall degree of conformance to the GIG Capstone Requirements Document. Where conformance cannot be achieved, appropriate rationale and associated risks (near, mid, and/or long term) should be presented.

7.2.3.2. Compliance with the DoD Information Enterprise Architecture (IEA)

The DoD Information Enterprise Architecture (IEA) V1.1 is focused on achieving net-centric information sharing. To comply with the DoD IEA V1.1, describe how each program approaches and implements net-centric features. Compliance does not require separate documentation; however, it does require that Program Managers and Sponsors/Domain Owners address, within existing architecture, analysis, and program architecture documentation, the issues identified by using the model. Furthermore, it requires that Program Managers and Sponsors/Domain Owners explicitly describe the path to net-centric information sharing that the program is taking.

The DoD IEA V1.1 provides specific guidance on compliance with the IEA.

7.2.3.3. Net-Centric Attributes

Combat Developers, DoD Agencies, and Program Managers should ensure acquisition programs adhere to the principles and rules described in the DoD Information Enterprise Architecture (IEA) V1.1. The Net-centric attributes table below outlines some key overarching characteristics of net-centric information sharing. However, the DoD IEA V1.1 should be used for the specifics.

Attribute	Description
Internet & World Wide Web Like	Adapting Internet & World Wide Web constructs & standards with enhancements for mobility, surety, and military unique features (e.g., precedence, preemption).
Secure & available information transport	Encryption initially for core transport backbone; goal is edge to edge; hardened against denial of service.
Information/Data Protection & Surety (built-in trust)	Producer/Publisher marks the info/data for classification and handling; and provides provisions for assuring authenticity, integrity, and non-repudiation.
Post in parallel	Producer/Publisher make info/data visible and accessible without delay so that users get info/data when and how needed (e.g., raw, analyzed, archived).

Smart pull (vice smart push)	Users can find and pull directly, subscribe or use value added services (e.g. discovery). User Defined Operational Picture vice Common Operational Picture.
Information/Data centric	Information/Data separate from applications and services. Minimize need for special or proprietary software.
Shared Applications & Services	Users can pull multiple applications to access same data or choose same apps when they need to collaborate. Applications on "desktop" or as a service.
Trusted & Tailored Access	Access to the information transport, info/data, applications & services linked to user's role, identity & technical capability.
Quality of Transport service	Tailored for information form: voice, still imagery, video/moving imagery, data, and collaboration.

Table 7.2.3.3.T1. Net-centric Attributes

7.2.3.4. Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))/DoD Chief Information Officer (CIO) Use of the DoD Information Enterprise Architecture (IEA)

The ASD(NII)/DoD CIO uses the DoD Information Enterprise Architecture (IEA) V1.1 in all three of the major decision processes of the Department.

The ASD(NII)/DoD CIO uses the DoD IEA V1.1 throughout the processes included in operating the Joint Capabilities Integration and Development System (JCIDS) to:

- Advise the Joint Requirements Oversight Council (JROC).
- Provide the basis for the development and refinement of joint enterprise and solution architectures by the Joint Staff and other DoD Components in support of the JCIDS.
- Develop assessments and provide recommendations to the Joint Requirements Oversight Council; the DoD IEA V1.1, including its concepts, products, data, conclusions, and implications provides a key source for these assessments.

The ASD(NII)/DoD CIO uses the DoD IEA V1.1 throughout the Planning, Programming, Budgeting and Execution (PPBE) process to:

- Review and provide recommendations for development of the Guidance for the Development of the Force and the Joint Programming Guidance.
- Provide recommendations to the Senior Level Review Group relating to Information Technology (IT) (including National Security Systems (NSS)), interoperability, and Information Assurance (IA).
- Review and evaluate Program Change Proposals and Budget Change Proposals relating to IT (including NSS), interoperability, and IA.

- Provide recommendations for Program Objective Memorandum planning and programming advice.

Finally, the ASD(NII)/DoD CIO uses the DoD IEA V1.1 throughout the Defense Acquisition Process to:

- Inform and support his recommendations as a member the Defense Acquisition Board and his decisions as the Milestone Decision Authority for delegated acquisition programs.
- Review Information Support Plans and evaluate the interoperability, interoperability key performance parameters, and information assurance aspects of those plans.

7.2.4. Integration into the Acquisition Life Cycle

7.2.4. Integration into the Acquisition Life Cycle

The following sections outline steps that the DoD Components, Combat Developers, Sponsors, Domain Owners, DoD Agencies, Program Managers, and/or other assigned managers should take to facilitate DoD Information Enterprise Architecture (IEA) V1.1 compliance and net-centric information sharing when acquiring Information Technology-enabled capabilities that will interoperate within the Global Information Grid.

Applicable to all three milestones, A, B, and C, architects should assure that any new architectural models they develop conform to the current version of the DoD Architecture Framework (DoDAF). The latest version of the DoDAF is always available on the DoD Architecture Registry System (DARS) website, URL https://dars1.army.mil/. Existing architecture models that require an update for reasons other than a DoDAF version change should include the updates necessary to conform with the most current DoDAF. Stable architecture models that do not otherwise require an update do not need to be updated solely because the DoDAF has changed. Also, IAW DoD policy, all AV-1s must be registered in the DARS. Instructions on how to do this are on the DARS portal.

7.2.4.1. Before Milestone A

Ensure that appropriate steps are taken to prepare or update a concept of operations and an operational view (High-level Operational Concept Description, OV-1) of the integrated (solutions) architecture for key mission areas and business processes using the DoD Architecture Framework (DoDAF) and the guidance in CJCS Instruction 6212.01, Enclosure E, paragraph 3. The Initial Capabilities Document (ICD) should reflect this architecture work, as prescribed by CJCS Instruction 3170.01 and in the format provided in the JCIDS Manual. It also supports analysis of alternatives, business process reengineering efforts, development of the acquisition strategy and acquisition information assurance (IA) strategy, and provides key artifacts that support development of the Information Support Plan. Ensure that integrated architectures adhere to the DoD net-centric strategies.

Ensure that the mandatory integrated architecture views conform to the DoD Information Enterprise Architecture (IEA) V1.1 and show linkage to parent enterprise architectures, where available, and within DoD Component and DoD-level Capability Portfolio Management architecture descriptions as they emerge.

The portion of the DoD IEA V1.1 that encompasses the "Use the Net-centric Environment" from the Net-Centric Operations and Warfare-Reference Model (NCOW-RM) provides a common taxonomy and lexicon for describing the use of Global Information Grid (GIG) services and capabilities and should be used in the development of activity models to describe the communications activities of systems that do not primarily provide services to the GIG. Systems that provide services to the GIG should use the portion of the DoD IEA V1.1 that describes service-oriented architecture to describe those system activities.

The DoD Information Enterprise Architecture (IEA) (version 1.1) is mandatory for any platform, program of record, system, subsystem, component, or application that conducts communications. To reduce architectural redevelopment, architecture from systems that were developed with older versions of the Net-Ready Key Performance Parameter (NR-KPP) should provide a mapping of those activities to the DoD IEA V1.1. For business systems, efforts should be made to align closely with the Business Enterprise Architecture.

Develop an Initial Capabilities Document to describe capability gaps identified through analysis of joint concepts and integrated (solutions) architectures. Use the criteria in CJCS Instruction 6212.01 to ensure the Initial Capabilities Document and supporting OV-1 address required interoperability standards.

7.2.4.2. Before Milestone B

Build or update the integrated architecture and supporting views (All Views, Capability Views, Data and Information Views, Operational Views, Project Views, Services Views, Systems Views, and Standards Views).

Develop a Capability Development Document, as prescribed by CJCS Instruction 3170.01 in the format provided in the JCIDS Manual, and a Net-Ready Key Performance Parameter (NR-KPP)

that address the interoperability and Information Assurance requirements described in CJCS Instruction 6212.01. Address issues associated with the updated integrated architecture, the Capability Development Document, and the DoD Information Enterprise Architecture (IEA) V1.1.

Use the required integrated architecture products to support development of the Information Support Plan.

Begin development of the Information Support Plan for Stage 1 Review. Use the criteria in CJCS Instruction 6212.01 to guide the acquisition of net-centric capabilities.

7.2.4.3. Before Milestone C

Update the integrated architecture and supporting views (All Views, Capability Views, Data and Information Views, Operational Views, Project Views, Services Views, Systems Views, and Standards Views) and ensure changes are reflected in the Capability Production Document, as prescribed by CJCS Instruction 3170.01 in the format provided in the JCIDS Manual, and in the Net-Ready Key Performance Parameter (NR-KPP). If the program is entering the acquisition process at Milestone C, develop a NR-KPP using guidance in CJCS Instruction 6212.01.

Address any remaining issues associated with mapping to the DoD Information Enterprise Architecture (IEA) V1.1, especially those related to Service-Level Agreements. A Service-Level Agreement defines the technical support, business parameters, and/or critical interface specifications that a service provider will provide to its clients. The agreement typically spells out measures for performance parameters and protocols used in interfacing, and consequences for failure.

Ensure the program delivers capabilities responsive to the Capability Production Document and meets interoperability and information assurance requirements reflected in the updated NR-KPP.

Use the criteria in CJCS Instruction 6212.01 to ensure services and data products delivered by the acquisition align with the Department's objectives for net-centricity.

Prepare and submit the Information Support Plan for final Stage 2 Review.

Address all information exchange requirements as part of the Information Support Plan and the Information Technology and National Security Systems Interoperability Certification processes.

7.2.4.4. After Milestone C and the Full-Rate Production Decision Review/Full-Deployment Decision Review

Continue life-cycle compliance with the Information Support Plan Interoperability Requirements Certification and the Information Technology and National Security System Interoperability Certification.

Continue life-cycle compliance with Information Assurance Certification and Accreditation.

7.2.5. DoD Enterprise Architecture-Related Guidance

7.2.5. DoD Enterprise Architecture-Related Guidance

The following paragraphs describe the major sources of guidance and tools related to the DoD Enterprise Architecture and supporting DoD strategies for implementing the architecture in information technology (including National Security Systems) programs. Program Managers and sponsors/domain owners should use the guidance, tools, and strategies outlined below throughout a program's life cycle to meet a variety of statutory and regulatory requirements.

7.2.5.1. DoD Architecture Framework (DoDAF)

The DoDAF provides a standard lexicon for architecture descriptions to insure a common denominator for understanding, comparing and integrating architecture descriptions. An integrated architecture consists of multiple views or perspectives (Operational View (OV), Systems View (SV), Technical Standards View (TV) and All View (AV)) that facilitate integration and promote interoperability across capabilities and among related integrated architectures.

The OV is a description of the tasks and activities, operational elements, and information exchanges required to accomplish DoD missions. The SV is a description, including graphics, of systems and interconnections providing for, or supporting, DoD functions. The TV is the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements. The AV products provide information pertinent to the entire architecture but do not represent a distinct View of the architecture. AV products set the scope and context of the architecture.

The Core Architecture Data Model (CADM) provides a lexicon for architecture information that promotes the exchange of information throughout Department. Typically the Combat Developer (or Domain Owner/Sponsor) will be responsible for the architecture description prior to Milestone B with the Program Manager taking on the responsibility subsequent to the approval at Milestone B.

7.2.5.2. DoD Information Technology (IT) Standards Registry (DISR)

The DoD IT Standards Registry is an online repository for a minimal set of IT standards to support interoperability. These standards are used as the "building codes" for all systems being procured in the DoD. Use of these building codes facilitates interoperability among systems and integration of new systems into the Information Enterprise. In addition, the DISR provides the capability to build profiles of standards that programs will use to deliver net-centric capabilities.

When building systems, requests for proposals (RFPs) and contract statements of work (SOWs) should be reviewed as part of approved acquisition processes to ensure IT standards established in Initial Capabilities Documents, Capability Development Documents, and Capability Production Documents are translated into clear contractual requirements. In addition, RFPs and contract SOWs should contain additional requirements for contractors to identify instances where cost, schedule, or performance impacts may preclude the use of IT standards mandated in DISR. Key net-centric elements that program architectures should focus on include:

- **Internet Protocol** – Ensure data packets are routed across network, not switched via dedicated circuits. Focus on establishing IP as the convergence layer.
- **Secure and Available Communications** – Encrypted initially for core network; goal is edge-to-edge encryption and hardened against denial of service. Focus is on Black (encrypted) Transport Layer to be established through the Transformational Communications Architecture implementation.
- **Assured Sharing** – Trusted accessibility to net resources (data, services, applications, people, devices, collaborative environment, etc). Focus on assured access for authorized users and denied access for unauthorized users.
- **Quality of Service** – Data timeliness, accuracy, completeness, integrity, availability, and ease of use. This is envisioned as being measured through the Net-Ready Key Performance Parameter. Focus on Service Level Agreements and service protocols with quality and performance metrics.

7.2.5.3. DoD Net-Centric Data and Services Strategy

The DoD Net-Centric Data Strategy provides the basis for implementing and sharing data in a net-centric environment. It describes the requirements for inputting and sharing data, metadata, and forming dynamic communities to share data. Program Managers (PMs) and Sponsors/Domain Owners should comply with the explicit requirements and the intent of this

strategy, which is to share data as widely and as rapidly as possible, consistent with security requirements. Additional requirements and details on implementing the DoD Data Strategy are found in section 7.4. (Refer to DoD Net-Centric Data Strategy, May 2003, issued by Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))/DoD Chief information Officer (CIO).).

The DoD Net-Centric Services Strategy (NCSS) reflects the DoD's recognition that a service-oriented approach can result in an explosion of capabilities for our warfighters and decision makers, thereby increasing operational effectiveness. A service-oriented approach can accelerate the DoD's ongoing effort to achieve net-centric operations by ensuring that our warfighters receive the right information, from trusted and accurate sources, when and where it is needed.

The DoD NCSS builds upon the DoD Net-Centric Data Strategy's goals of making data assets visible, accessible, and understandable. This strategy establishes services as the preferred means by which data producers and capability providers can make their data assets and capabilities available across the DoD and beyond. It also establishes services as the preferred means by which consumers can access and use these data assets and capabilities.

The DoD's vision is to establish a Net-Centric Environment (NCE) that increasingly leverages shared services and Service Oriented Architecture (SOA) that are:

- Supported by the required use of a single set of common standards, rules, and shared secure infrastructure provided by the Enterprise Information Environment Mission Area (EIEMA);
- Populated with appropriately secure mission and business services provided and used by each Mission Area;
- Governed by a cross-Mission Area board, which is chaired by the DoD CIO;
- Managed by Global information Grid (GIG) Network Operations (NetOps).

When this vision is achieved, all members of the DoD will realize significant benefits. A common infrastructure enables force capabilities to be readily networked in support of joint warfighting and operations. Interoperability of capabilities is improved when Military Departments, Agencies, and mission partners create reusable "building blocks" through the use of services. The coordinated management of this environment under GIG NetOps provides the necessary situational awareness for joint forces to use the capabilities that are available. The DoD's commitment to govern this evolution will greatly improve the ability to respond to evolving operations and missions. (Refer to: DoD Net-Centric Services Strategy, Strategy for a Net-Centric, Service Oriented DoD Enterprise, March, 2007, issued by ASD(NII)/DoD CIO.)

To assist in achieving the net-centric information sharing vision, PMs should be cognizant of the following principles from the DoD Information Enterprise Architecture (IEA) V1.1 that address the deployment of data and services:

- Data, services and applications belong to the DoD Enterprise. Information is a strategic asset that must be accessible to the people who need it to make decisions.
- Data, services, and applications should be loosely coupled to one another. The interfaces for mission services that an organization provides should be independent of the underlying implementation. Likewise, data has much greater value if it is visible, accessible and understandable outside of the applications that might handle it.
- Only handle information once (the "OHIO" principle). Information that exists should be reused rather than recreated.
- Semantics and syntax for data sharing should be defined on a community basis. Information sharing problems exist within communities; the solutions must come from within those communities.
- Data, services and applications must be visible, accessible, understandable, and trusted to include consideration of "the unanticipated user". All needs can never be fully anticipated. There will inevitably be unanticipated situations, unanticipated processes, and unanticipated partners. By building capabilities designed to support users outside of the expected set, the Department can achieve a measure of agility as a competitive advantage over our adversaries.
- Enterprise Services providing data or information shall be authoritative and, thus, trusted as being accurate, complete and having assured integrity. Authoritative information has a pedigree that can be traced to a trusted source.
- Enterprise Services must be hosted in environments that meet minimum GIG computing node standards in terms of availability, support and backup. A small set of Enterprise Services, designated as Core Enterprise Services, are mandated for DoD-wide use by the ASD(NII)/DoD CIO in order to provide enterprise-wide awareness, access and delivery of information via the GIG.

Refer to: DoD Information Enterprise Architecture (IEA) V1.1 issued by ASD(NII)/DoD CIO.

7.2.5.4. DoD Information Assurance (IA) Strategic Plan

The DoD IA Strategic Plan defines an enterprise-wide strategic direction for assuring information and guides planners, programmers, strategists and organizational leaders. The Net-Centric Enterprise IA Strategy serves as an annex to the DoD IA Strategic Plan, and focuses specifically on amplifying the goals and approaches for transforming to the IA essential to safeguarding a net-centric information environment.

The Net-Centric Enterprise IA Strategy is a driver for the IA Component of the Global information Grid (GIG) Integrated Architecture. The Net-Centric IA Strategy describes the DoD strategy for integration of IA into the global, net-centric information environment. The end-to-end IA component of the GIG is comprised of a set of informational documents and DoD Architecture Framework (DoDAF) products (tools) that define IA constructs as conceptualized and specified for integration of IA into the net-centric information environment in support of a secure, globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on

demand to warfighters, defense policymakers, and support personnel. The intent of the Net-Centric IA Strategy is to reflect an approach to IA concepts and definitions from a "services" point-of-view instead of a "system" point-of-view, without specifying requirements related to specific implementations or architectures.

For more detail about Information Assurance, see Section 7.5.

7.2.5.5. Global Information Grid (GIG) Enterprise Services (GIG ES) Capability Development Document

The GIG ES Capability Development Document is currently focused on nine core enterprise services to be provided by the Net Centric Enterprise Services (NCES) Program. These services are the foundation for the initial net-centric capabilities to be provided by the Defense Information Systems Agency. The Capability Development Document describes the overall set of services in detail.

The NCES program will develop the core enterprise services incrementally. The NCES Program Plan describes the increments and their anticipated schedule. Each program that is dependent upon the core services being developed by the NCES program should address the impact of the incremental NCES schedule on their program.

7.3. Interoperability and Supportability of Information Technology and National Security Systems

7.3.1. Interoperability and Supportability

Interoperability is the ability of systems, units, or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. Information Technology (IT) and National Security Systems (NSS) interoperability includes both

the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations and missions over the life cycle, and it should be balanced with IA.

Supportability for IT systems and NSS is the ability of systems and infrastructure components, external to a specific IT or NSS, to aid, protect, complement, or sustain the design, development, testing, training, or operations of the IT or NSS to achieve its required operational and functional capabilities.

7.3.2. Mandatory Policies

7.3.2.1. DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"

- Section 4.1 of this Directive requires IT and NSS employed by U.S. Forces to interoperate with existing and planned systems and equipment of joint, combined and coalition forces and with other U.S. Government Departments and Agencies, as appropriate (based on capability context).
- Section 4.3 requires that IT and NSS interoperability and supportability needs, for a given capability, be identified through:
    - The Defense Acquisition System (as defined in the DoD 5000 series issuances);
    - The Joint Capabilities Integration and Development System process;
    - The Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF) change recommendation process (see CJCSI 3180.01, Joint Requirements Oversight Council (JROC) Programmatic Processes for Joint Experimentation and Joint Resource Change Recommendations).

- Section 4.5 provides that IT and NSS interoperability be verified early, and with sufficient frequency throughout a system's life, or upon changes affecting interoperability or supportability, to assess, evaluate, and certify its overall interoperability and supportability within a given capability. Joint interoperability certification testing shall be as comprehensive as possible, while still being cost effective, and shall be completed prior to fielding of a new IT and NSS capability or upgrade to existing IT and NSS.
- Section 4.8 requires that interoperability and supportability needs be balanced with requirements for Information Assurance (IA).

7.3.2.2. DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"

Extracts:

- *E3.1.5. A Net-Ready Key Performance Parameter (NR-KPP), consisting of verifiable performance measures and metrics, shall be used to assess information needs, information timeliness, IA, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. A NR-KPP shall be defined for all IT and NSS defense acquisition and procurement programs and shall be specified to a level of detail that allows verification of interoperability throughout a system's life. The defined NR-KPP shall be developed so that it can be reliably measured, tested and evaluated.*
- *E3.1.6. IT and NSS interoperability and supportability needs shall be managed, evaluated, and reported over the life of the system using an Information Support Plan (ISP) . For all DoD ACAT programs and non-ACAT acquisitions and procurements, a ISP shall be produced and used to analyze interoperability and supportability requirements specified in the NR-KPP. . . .*
- *6.2.3.6.1. All IT and NSS, regardless of ACAT, must be tested for interoperability before fielding and the test results evaluated and systems certified by the DISA (JITC). IT and NSS interoperability test and evaluation shall be conducted throughout a system's life, and should be achieved as early as is practical to support scheduled acquisition or procurement decisions. Interoperability testing may be performed in conjunction with other testing (i.e., DT&E, OT&E, early-user test) whenever possible to conserve resources.*
- *6.2.3.6.2. IT and NSS interoperability testing can occur in multiple stages. Evolutionary acquisitions or procurements, and normal life-cycle modifications, result in a progressively more complete capability. Therefore, there may be instances when it is important to characterize a system's interoperability before all critical interface requirements have been tested and certified. However, all critical interfaces, identified in the NR-KPP, which have been tested, must be successfully certified for interoperability prior to fielding. When appropriate (e.g., between successful completion of OT and the*

fielding decision), the DISA (JITC) shall issue interim interoperability certification letters specifying which of the system's interoperability needs have been successfully met and which have not. The DISA (JITC) shall issue an overall system certification once the system successfully meets all requirements of the NR-KPP validated by the Chairman of the Joint Chiefs of Staff. The DISA (JITC) shall provide interoperability certification letters to the USD(AT&L), the USD(C)/CFO, the ASD(NII)/DoD CIO, the DPA&E, the DOT&E, the Chairman of the Joint Chiefs of Staff, and the Commander, USJFCOM, as well as to the OTA and program manager, as applicable.

7.3.2.3. DoD Directive 5000.01, "The Defense Acquisition System"

- Paragraph E1.1.10 establishes the requirement to acquire systems and families of systems that are interoperable.
- Paragraph E1.1.11 states the requirement that test and evaluation shall assess interoperability.
- Paragraph E1.1.16 cites interoperability as a primary reason for acquisition managers to consider and use performance-based strategies for acquiring and sustaining products and services.

7.3.2.4. DoD Instruction 5000.02, "Operation of the Defense Acquisition System"

Extracts:

- *Enclosure 6, paragraph 2.c.(8) states: Interoperability Testing: All DoD MDAPs, programs on the OSD T&E Oversight list, post-acquisition (legacy) systems, and all programs and systems that must interoperate, are subject to interoperability evaluations throughout their life cycles to validate their ability to support mission accomplishment. For IT systems (including NSS) with interoperability requirements, the Joint Interoperability Test Command (JITC), regardless of ACAT, shall provide system interoperability test certification memorandums to the Deputy Under Secretary of Defense (Acquisition and Technology) (DUSD(A&T)), the ASD(NII)/DoD CIO, and the Director, Joint Staff J-6, throughout the system life-cycle.*
- *Enclosure 6, paragraph 3 states: During DT&E, the materiel developer shall:*
  - d. Assess technical progress and maturity against critical technical parameters, to include interoperability, documented in the TEMP; and
  - h. In the case of IT systems, including NSS, support the DoD Information Assurance Certification and Accreditation Process and Joint Interoperability Certification process; . . .

7.3.2.5. CJCS Instruction 6212.01, "Interoperability and Supportability of Information Technology and National Security Systems"

This publication provides instruction and checklists to implement DoD Directive 4630.5 and DoD Instruction 4630.8.

7.3.3. Interoperability and Supportability Integration into the Acquisition Life Cycle

CJCS Instruction 6212.01, dated 15 December 2008, includes a figure that provides insights into the relationship between key interoperability and supportability activities and the Joint Capabilities Integration and Development System and Defense Acquisition processes. The figure is outdated, as it reflects the acquisition process prior to the re-issued DoD Instruction 5000.02 published 8 December 2008.

7.3.4. Net-Ready Key Performance Parameter (NR-KPP)

7.3.4. Net-Ready Key Performance Parameter (NR-KPP)

The Net-Ready Key Performance Parameter (NR-KPP) has been developed to assess net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP replaces the Interoperability KPP, and incorporates net-centric concepts for achieving Information Technology (IT) (including National Security Systems (NSS)) interoperability and supportability. The NR-KPP assists Program Managers (PMs), the test community, and Milestone Decision Authorities in assessing and evaluating IT (including NSS) interoperability.

The NR-KPP assesses information needs, information timeliness, Information Assurance (IA), and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP consists of verifiable performance measures and associated metrics required to evaluate the timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability. PMs will use the NR-KPP documented in Capability Development Documents and Capability Production Documents to analyze, identify, and describe IT (including NSS) interoperability needs in the Information Support Plan and in the test strategies in the Test and Evaluation Master Plan. The following elements comprise the NR-KPP:

- Supporting integrated architecture products, including the Joint Common Systems Function List required to assess information exchange and operationally effective use for a given capability;
- Compliance with DoD Net-centric Data and Services strategies, including data and services exposure criteria;
- Compliance with applicable Global information Grid (GIG) Technical Direction to include DoD IT Standards Registry-mandated GIG net centric IT Standards reflected in the Technical Standards View-1 and, Functional and Technical Implementation of GIG Enterprise Service Profiles necessary to meet the net centric operational requirements specified in the integrated architecture system views;
- Verification of compliance with DoD IA requirements; and
- Compliance with Supportability elements to include Spectrum Analysis, Selective Availability Anti-Spoofing Module, and the Joint Tactical Radio System.

7.3.4.1. Supporting Integrated Architecture Views and Compliance

In accordance with the DoD 4630 Series, integrated architecture products or views defined in DoD Architecture Framework Version 1.5 or Version 2.0 (and related discussion in DoD Instruction 4630.8) shall be used to assess information exchange and use for a given capability. The functional proponent, domain owner, Principal Staff Assistant, and Program Manager (PM) use the supporting integrated architecture products or views in developing the Net-Ready Key Performance Parameter and preparing the Information Support Plan.

PM compliance with required supporting integrated architecture views is demonstrated through inspection and analysis of developed architecture views to determine conformance with DoD Architecture Framework specifications and that all required views have been produced. CJCS Instruction 3170.01 and CJCS Instruction 6212.01 requirements apply.

7.3.4.2. DoD Net-Centric Data Strategy

Compliance with the DoD Directive 8320.02, "Data Sharing in a Net-Centric Department of Defense" and the DoD Net-Centric Data Strategy is an essential prerequisite of net-centric operations. In order for a program to gain Interoperability and Supportability Certification, program data and services must be "exposed" by making data elements and provided services visible, accessible, and understandable to any potential user with access to the GIG, both anticipated and unanticipated.

Verification of compliance with the DoD Net-Centric Data Strategy and DoD Net-Centric Services Strategy will be accomplished through the analysis of the sponsor-provided architecture and verification products with accompanying text detailing the program's compliance strategy. Documentation (in integrated architecture products or other forms) must clearly identify all net-centric services and data as adopted from Universal Core, Domain Cores, and COIs.

- In addition to the architecture products, sponsors must complete Exposure Verification Tracking Sheets to self-evaluate compliance with the direction in the exposure directives.
- A guide for selecting which type of Tracking Sheet is required for each program and instructions for the completion of each type is located on the CJCSI 6212 Resource Page.

7.3.4.3. Global Information Grid (GIG) Technical Guidance (GTG)

The GTG is an evolving web enabled capability providing the technical guidance necessary for an interoperable and supportable GIG built on Net-Centric principles. The GTG provides a one-stop, authoritative, configuration managed source of technical compliance guidance that synchronizes previously separate efforts. The GTG is designed to enable users to decide which guidance is applicable and to find detailed information and artifacts needed to meet functional requirements (GIG features and capabilities), DoD Information Technology (IT) Standards Registry (DISR)-mandatory GIG net-centric IT standards, supporting GIG IT standards, and GIG Enterprise Service Profiles (GESPs).

The GTG is the source for all technology guidance and standards implementation information used in describing GESPs necessary to meet the net centric operational requirements specified in the system/service views of an integrated architecture. The GTG contains a program characterization questionnaire and compliance declaration matrix that points to applicable GESPs. The GESPs are built from DISR mandated IT Standards reflected in a standards profile and include associated implementation guidance reference architecture and testing criteria necessary to meet all GIG related requirements characterized in the integrated architecture system/service views. GTG Content includes:

- The GTG is designed to enable users to decide which guidance is applicable and to find detailed information and artifacts on:
    - Associated technical functional requirements (GIG features and capabilities);
    - DISR mandatory GIG net-centric IT standards;
    - Supporting GIG IT standards;
    - Associated profiles;
    - Reference implementations; and
    - Test criteria.
- The GTG contains a program characterization questionnaire and compliance declaration matrix that points to applicable GIG Enterprise Service Profiles (GESPs). The GESPs are aligned with the DoD IEA V1.1 and are determined based on if following criteria capability:
    - Spans organizational boundaries;
    - Is mandatory or mission critical across the GIG Enterprise;
    - Can be characterized in a GIG Enterprise Standards Profile;
    - Is essential for resolving GIG end-to end interoperability issues;
    - Enables net centric information sharing for multiple acquisition programs; and
    - Is important from a security perspective.

Program Manager compliance with applicable GTG is demonstrated through inspection of Joint Capabilities Integration and Development System documentation and test plans, and during Joint Interoperability Test Command interoperability certification testing (see CJCS Instruction 3170.01 and CJCS Instruction 6212.01 for detailed discussions of the process).

7.3.4.4. Compliance with DoD Information Assurance (IA) Requirements

DoD IA requirements, including IA certification and accreditation, are specified in DoD Directive 8500.01, DoD Instruction 8500.2, DoD Directive 8581.1, and DoD Instruction 8510.01. Satisfaction of these requirements results in system accreditation and the issuance of an authorization to operate. See section 7.5 for details.

7.3.5. Net-Ready Key Performance Parameter (NR-KPP) Compliance Checklist

7.3.5. Net-Ready Key Performance Parameter (NR-KPP) Compliance Checklist

The following checklist summarizes the requirements for demonstrating compliance with the NR-KPP and should be useful in preparing for milestone approvals:

7.3.5.1. Required Documentation

Does the capability have the following required documentation?

- Applicable Integrated Architecture Products, AV-1, OV-2, OV-4, OV-5, OV-6c, SV-4, SV-5, SV-6 DISR Standards Compliance with draft TV-1.
- Compliant with Net-Centric Data Strategy and Net-Centric Services Strategy, Data Exposure Verification Tracking Sheets.
- Applicable GTG citations, GTG statements, and the corresponding DISR-Mandated GESP IT Standards included in the program manager's TV-1 as necessary to meet the net-centric operational characterized in the integrated architecture system views.

- IA requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an accreditation decision by the Designated Approval Authority.
- Applicable Supportability requirements to include SAASM, Spectrum and Joint Tactical Radio System requirements (see section 7.6).

7.3.5.2. Supporting Integrated Architecture Products

- Have all architecture products been developed in accordance with the DoD Architecture Framework (DoDAF)?
- Does the AV-1 describe a net centric environment? (Note: If this is a non-net-centric environment, i.e., a legacy network, make sure that is noted in the architecture.)
- Has the TV-1 been prepared using applicable information technology standards profiles contained in the DISR?
- Have all the interfaces listed in the OV-2 and SV-6 been appropriately labeled with the GIG core enterprise services needed to meet the requirements of the applicable capability integrated architecture?
- Have specific capability integrated architecture OV-6c time event parameters been correlated with GIG architecture OV-6c?
- Have verifiable performance measures and associated metrics been developed using the integrated architectures, in particular, the SV-6?

7.3.5.3. Global Information Grid (GIG) Technical Guidance (GTG) Compliance

The GTG has a compliance regime with granularity appropriate to the Milestone phase or maturity of a program.

- At Milestone B, Capability Development Documents/Information Support Plans (ISPs) will include a preliminary declaration of the functional implementation features and technical capabilities and identify which technical implementation profiles are applicable. Draft TV-1's and TV- 2's will also be included.
- At Milestone C, Capability Production Documents/ISPs and post Milestone C Tailored Information Support Plans will include the final declaration of functional implementation and technical features, identify technical implementation profiles, and complete final TV-1s and TV-2s. The completeness and sufficiency of the program's citing of artifacts drawn from the GTG in determining net readiness will be assessed and certified by Joint Staff J-6 in the ISP. A final declaration of selected emerging or maturing standards not found in the DoD Information Technology Standards Registry with rationales and risks will be included.

7.3.5.4. Information Assurance (IA)

- Have applicable IA requirements of DoD 8500 series issuances and Director of Central Intelligence Directives been identified?
- Is the system level IA design (to include the use of enterprise services) in alignment with the IA component of the Global Information Grid integrated architecture?
- Has the applicable capability (system) received an authorization to operate (ATO) from the appropriate Designated Accrediting Authority?

7.3.5.5. Compliance with Spectrum Supportability

Spectrum Supportability Policy and Electromagnetic Environmental Effects (E3) control are contained in DoD Instruction 4650.01, "Policy and Procedures for Management and Use of the Electromagnetic Spectrum."

The spectrum supportability process includes national, international, and DoD policies and procedures for the management and use of the electromagnetic spectrum. The Capability Development Document/Capability Production Document must document the following:

- Permission has been (or can be) obtained from designated authorities of sovereign ("host") nations (including the United States) to use that equipment within their respective borders; and the newly acquired equipment can operate compatibly with other spectrum-dependent equipment already in the intended operational environment (electromagnetic compatibility).
- All Information Technology, including National Security Systems, must comply with DoD Instruction 4650.01 (see also section 7.6).

7.3.6. Information Support Plan (ISP), Enhanced Information Support Plan (EISP), and Tailored Information Support Plan (TISP)

7.3.6.9. Tailored Information Support Plan (TISP) Instructions

7.3.6.10. Information Support Plan (ISP) Waiver Process

7.3.6. Information Support Plan (ISP), Enhanced Information Support Plan (EISP), and Tailored Information Support Plan (TISP)

The Information Support Plan (formerly called the Command, Control, Communication, Computers, and Intelligence Support Plan (C4ISP)) is intended to explore the information-related needs of an acquisition program in support of the operational and functional capabilities the program either delivers or contributes to. Information Support Plans (ISPs) provide a means to identify and resolve potential information support implementation issues and risks that, if not properly managed, will limit or restrict the ability of a program to be operationally employed in accordance with the defined capability. The ISP focuses on net-readiness, interoperability, information supportability, and information sufficiency concerns. The ISP process is one of discovery, requiring analysis of the program's integrated architecture and processes associated with meeting a capability. This analysis identifies information need, net-centric, interoperability, and supportability issues and assesses compliance with Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer information policy and goals.

The ISP comes in several forms as a document (ISP or TISP) or as data in the form of an EISP tool (for both ISP and TISPs). The preferred and future mandatory format is using the data-centric EISP tool. The EISP is evolving to the only form for ISP content. The ISP provides the Program Manager (PM) a mechanism to identify his/her information-related dependencies, to manage these dependencies and to influence the evolution of supporting systems to meet the demands of the system as it evolves to meet the warfighter's needs and capabilities. In the case where the supporting system will not be available, the ISP should provide the PM with awareness of this problem in sufficient time to adjust the program in the most cost effective and operationally efficient manner.

The end-product of the ISP/EISP/TISP is the identified issues and risks associated with information needs and dependencies of the program. Information issues and risks should be treated as any program issue or risk as defined in the AT&L's "Risk Management Guide for DoD Acquisition, Sixth Edition, Version 1, August, 2006." Information issues and risks should be managed as defined in this guide and presented in acquisition decision meetings (such as Overarching Integrated Product Team meetings) by the PM as any other area of issue and risk is presented (e.g., reliability risks).

The Command, Control, Communication, Computers, and Intelligence Support Plan has evolved into the ISP as a result of the revision of the CJCS Instruction 3170.01 requirements documentation. Joint Capabilities Integration and Development System documents: Initial Capabilities Document, Capability Development Document, and Capability Production Document are required to successfully complete an ISP. The ISP will use the integrated

architecture from the system as a key reference document and focus on analysis of this architecture.

7.3.6.1. Review of Information Support Plan (ISP)-Specific Mandatory Policies

- DoD Instruction 5000.02, Enclosure 4, Table 3, "Regulatory Requirements Applicable to All Acquisition Programs," requires that all acquisition programs (except Defense Space Acquisition Board-governed programs as noted below), regardless of acquisition category level, submit an ISP at Milestones B (Initial ISP), CDR (Revised ISP), Milestone C (ISP of Record, unless waived), at major system or software updates (Updated ISP), and at Program Initiation for ships (Initial ISP).
- National Security Space Acquisition Policy, Number 03-01, requires Defense Space Acquisition Board-governed programs to submit an ISP.
- DoD Instruction 4630.8, Enclosure 4 provides a mandatory ISP format.
- CJCS Instruction 6212.01 also provides detailed implementing guidance regarding the ISP and specifically the TISP.

7.3.6.2. Information Support Plan (ISP) Integration into the Acquisition Life Cycle

7.3.6.2. Information Support Plan (ISP) Integration into the Acquisition Life Cycle

An ISP provides the methodology for meeting a program's information needs and managing the issues and risks associated with those need. It ensures compliance with Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) policy and is used by various other activities to monitor compliance and sufficiency. The Joint Staff utilizes the ISP in the Interoperability and Supportability

Certification process; J2 utilizes the ISP for intelligence supportability (CJCS Instruction 3312.01); and the ISP is used as part of Title 40/CCA statutory oversight, oversight of Information Assurance (IA), spectrum supportability, and the National Signature Program.

The ISP is a living document or living data for the Enhanced Information Support Plan (EISP), which is developed over the life cycle of a program. At each point of review, the ISP builds and follows the information needs required by a program to meet its intended capability(ies). A completed ISP answers the following seven questions for information needed to support the operational/functional capability(ies) of a system.

- What information is needed?
- How good must the information be?
- How much information (needed or provided)?
- How will the information be obtained (or provided)?
- How quickly must it be received in order to be useful?
- Is the information implementation net-centric?
- Does it comply with DoD information policies?

There are three ISP development approaches during the life cycle:

1. A traditional ISP Document for Acquisition Category (ACAT) I, IA, and designated ISP Special Interest Programs (see (Office of the ASD(NII) (OASD(NII) Memorandum, Subject: "2007 Information Support Plan (ISP)/Command, Control, Communications, Computers, and Intelligence (C4I) Support Plan Special Interest List," May 30, 2007). The Information Needs and Discovery Process will continue to follow the 13 steps in DoD Instruction 4630.8, Enclosure 4 plus the addition of a Net-Ready Key Performance Parameter analysis.
2. A data-centric ISP (EISP) for ACAT I, IA, and designated ISP Special Interest Programs, using an Extensible Markup Language (XML)-based ISP data collection tool provided by OASD(NII)/Deputy CIO (DCIO) and an associated data converter that generates a properly formatted ISP document from the data. This relieves the ISP developer from needing to produce and format a written ISP document and sets the stage for other options of analysis and presentation of ISP data.
3. Tailored ISP (TISP) Document for ACAT II and below programs (including ISP Special Interest) and non-ACAT programs that receive Joint Staff (JS) J-6 approval may use this method. These programs may tailor the content of their ISP per the procedures in section 7.3.6.9. Authorized programs can obtain a final decision from the JS J-6 for their tailored plan to include any special needs identified by the JS (J-2 and J-6) for the intelligence and supportability/interoperability certification processes required by CJCS Instruction 3312.01 and CJCS Instruction 6212.01. The final DoD Component approved plan (TISP) will be submitted to OASD(NII)/DCIO ISP document repository (via the Defense Information Systems Agency-managed Joint C4I Program Assessment Tool - Enhanced (JCPAT-E) tool (site requires certificate and/or login)).

The ISP development process serves to guide an ISP throughout a program's acquisition life cycle as opposed to creating a discrete document at each major acquisition decision point. In support of acquisition decisions, the ISP will be submitted for review at four points during the acquisition cycle. Names have been assigned to ISPs for each stage of development (i.e. Initial ISP, Revised ISP, Final ISP of Record, and Updated ISP). Programs under the Defense Space Acquisition Board (DSAB) follow different milestone events as shown in Figure 7.3.6.2.F1, but also build towards a final ISP of Record.

ISPs for ACAT I, IA programs, and ISPs or TISPs for Special Interest programs will undergo a complete OSD-level review. ISPs or TISPs for all other ACAT II and below programs and Non-ACAT programs will be reviewed using the JS(J-6) review process as described in CJCSI 6212.01.

Figure 7.3.6.2.F1, "ISP Submission Timeline," illustrates when ISPs must be submitted to the JCPAT-E tool. It depicts when ISP reviews occur and lists the activities associated with each review. All OSD level ISP reviews and J-6-level ISP reviews will be completed within thirty calendar days of posting with the exception of a final acceptance review by the J-2 and J-6 which will last 15 calendar days. See outline below for the review of time frames and potential responses:

Review time frames:

- 30 Calendar Days: OSD or J-6-level Review
- N Calendar Days: Program Manager (PM) response preparation (N = time determined by PM)
- 15 Calendar Days: Validation of PM responses by OSD/J-6 for MS C ISP of Record or Updated ISP
- 30 Calendar Days: Submission of ISP of Record signed by Component to JCPAT-E Document Repository

OSD or J-6 Responses:

- Initial ISP/TISP: Acceptance Memorandum from NII /or JS for TISP
- Revised ISP/TISP: Acceptance Memorandum from NII/ or JS for TISP
- ISP/TISP of Record: Acceptance of a Component Approved ISP/TISP Memorandum from NII/ and/or JS Interoperability Certification
- Updated ISP/TISP: Acceptance of a Component Approved ISP/TISP Memorandum from NII/ and/or JS Interoperability Certification

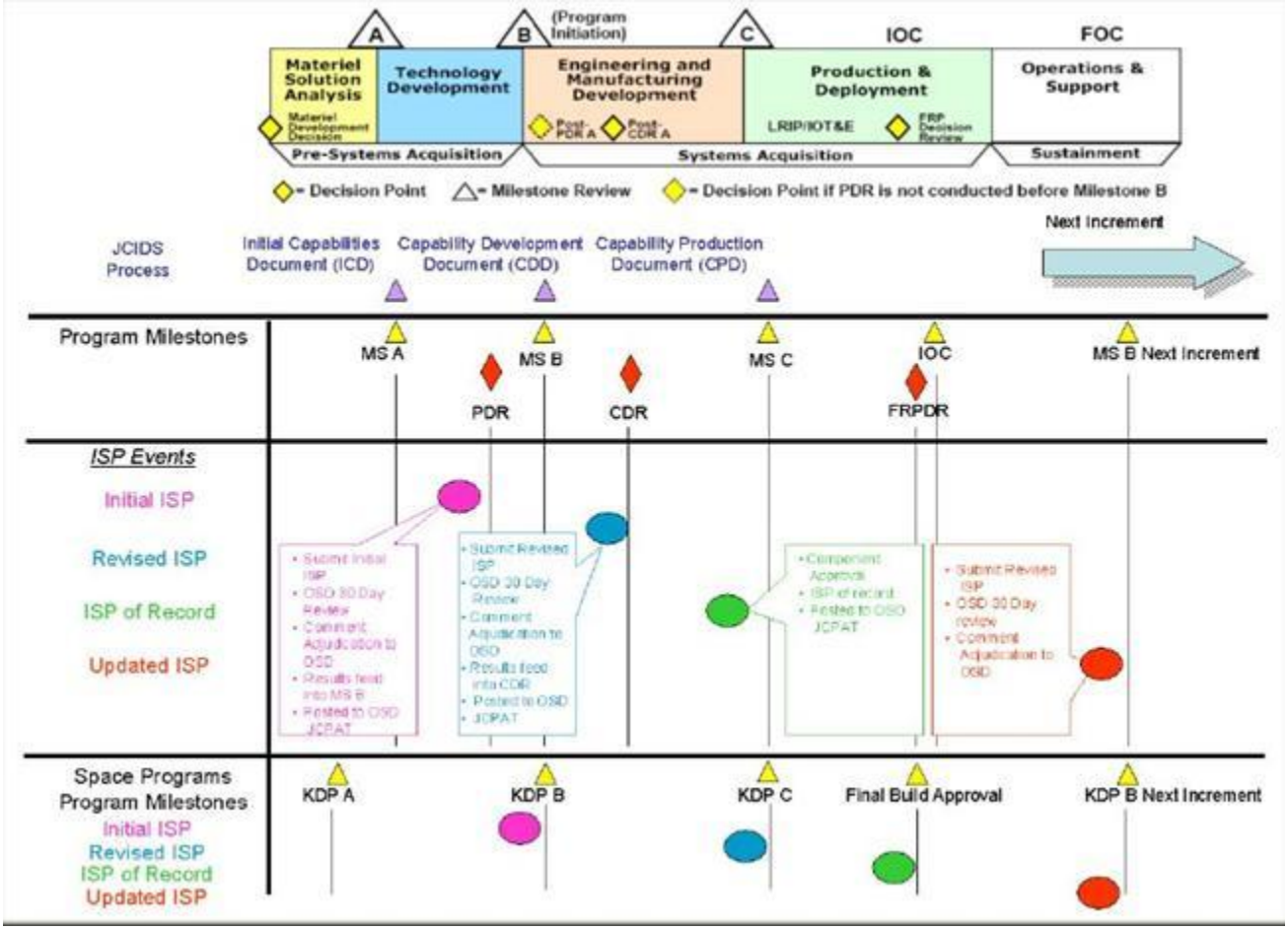


Figure 7.3.6.2.F1. ISP Submission Timeline

1. An Initial ISP (TISP for eligible programs) is completed by all acquisition programs prior to MS B. The Initial ISP's content emphasizes the system's functional design and the operational and technical architecture view analysis. A program's Initial ISP should be posted on JCPAT-E in sufficient time to permit completion of a 30 day review, plus comment adjudication period prior to the program's pre-MS B Overarching Integrated Product Team (OIPT). ISP reviewers will issue comments in the form of a Comment Resolution Matrix (CRM) or submit them directly into the JCPAT-E tool. During the comment adjudication period, the PM should contact each commenter to resolve issues before the completed CRM is reposted to the JCPAT-E with concurrence by JS J-6.

   For ACAT I and IA, and ISP Special Interest Programs: Initial ISP Acceptance Memorandum from OASD(NII) or JS will be provided to the PM and DoD Component via JCPAT-E. Information related issues and risks annotated as "Critical" (i.e., have operational relevance) discovered during ISP analysis and within the review process will be addressed by the PM within the risk assessment portion of the OIPT briefing. For

ACAT II programs and below and Non-ACAT programs: Initial ISP completion status will be emailed from JS J-6 to the PM.

2. A Revised ISP is completed prior to Critical Design Review (CDR) (or equivalent event). Programs with multiple CDRs should coordinate Revised ISP submissions with OASD(NII)/DCIO. Revised ISP content should emphasize identification of the program's information dependencies, through analysis of the program's operational, system, and technical architecture views.

   A Revised ISP should be developed by the PM and submitted along with an adjudicated CRM from the previous review to OASD(NII)/DCIO via the JCPAT-E. Submission must be made to allow time for completion of a 30-day review, plus comment adjudication period prior to CDR. During the comment adjudication process; the PM should coordinate responses with each comment submitter. A completed comment resolution matrix must be submitted to JCPAT-E prior to CDR. Following completion of the Revised ISP review an Acceptance Memorandum from NII or JS will be provided to the PM and Component via JCPAT-E. Information issues and risks discovered in the analysis associated with producing the ISP and in the review process will be addressed by the PM in his risk assessment briefing during the program's CDR.
3. A Final ISP of Record is completed prior to MS C unless otherwise determined by OASD(NII)/DoD CIO. A Final ISP should be developed by the PM and shall be submitted along with the Adjudicated CRM from the previous review to OASD(NII)/DCIO via the JCPAT-E. After completion of a 30-day review and subsequent comment adjudication period, an additional 15-day final review (CRM acceptance) will be conducted by J-2 and J-6. The purpose of this acceptance review will be to issue intelligence certifications and interoperability and supportability certifications as required in CJCS Instructions 3312.01 and 6212.01. Upon receipt of the Joint Staff J-2 and J-6 certifications, the final DoD Component-approved ISP (signed by the DoD Component Approval Authority) will be submitted into JCPAT-E as the Final ISP of Record. An Acceptance Memorandum from OASD(NII) or JS will be provided to the PM and DoD Component, via JCPAT-E, to document completion of this ISP version. The Final ISP of Record must be available to the Joint Interoperability Test Command prior to Interoperability Test Certification.
4. An Updated ISP can be of two types: (1) an ISP submitted to update the document posted on the JCPAT-E tool (requires no formal reviews), or (2) an updated ISP version that is provided for the next program increment or upgrade beyond MS C. In this case, if there are multiple follow-on milestones, the ISP will be submitted for review prior to MS B, CDR and MS C as shown above. If an upgrade pertains only to a single MS decision point, as is frequently the case with software revisions to an IT program, then the following procedures for a Final ISP of Record will be used. An Acceptance Memorandum from OASD(NII) or JS will be provided to the PM and DoD Component via JCPAT-E upon completion of the Updated ISP.

The following paragraphs describe the ISP-related actions that PMs should take in each acquisition phase. Figure 7.3.6.2.F1 describes the ISP activities at each milestone by program

situation. The EISP is recommended as the preferred product and is migrating to become the mandatory product.

7.3.6.2.1. Before Milestone A

While the ISP is not required until MS B, early development of the ISP will assist in development of the program's integrated architecture and Concept for Operations discussed in the CJCS Instruction 3170.01. Beginning development of the EISP early will help define information needs and dependencies for the program.

7.3.6.2.2. Before Milestone B (or program initiation for ships) (KDP B for Space Programs)

- Define all information needs and related-dependencies according to DoD Instruction 4630.8, CJCS Instruction 6212.01, CJCS Instruction 3170.01, and the JCIDS Manual to ensure information supportability is addressed in the Information Support Plan (ISP) and Capability Development Document.
- Submit the ISP for formal, coordinated, Initial ISP Review according to DoD Instruction 4630.8 and Pilot Memorandum, OASD(NII), "Information Support Plan (ISP) Acquisition Streamlining Pilot Program," August 26, 2005 (Available to users in the ".Mil" domain at the JCPAT-E site under "ASD (NII)/DoD CIO ISP Pilot Memo and Special Interest List").

7.3.6.2.3. Before CDR (KDP C for Space Programs)

- Update all information needs and related-dependencies according to DoD Instruction 4630.8, CJCS Instruction 6212.01, CJCS Instruction 3170.01, and the JCIDS Manual to ensure information supportability is addressed in the Information Support Plan (ISP) and Capability Production Document.
- Submit the ISP for formal Review according to DoD Instruction 4630.8 and Pilot Memorandum, OASD(NII), "Information Support Plan (ISP) Acquisition Streamlining Pilot Program," August 26, 2005 (Available to users in the ".Mil" domain at the JCPAT-E site under "ASD (NII)/DoD CIO ISP Pilot Memo and Special Interest List.").
- Results of the Critical Design Review should be used by the Program Manager in making decisions prior to contract award.

7.3.6.2.4. Before Milestone C (Final Build Approval for Space Programs)

DoD Instruction 4630.

- Update all information needs and related-dependencies according to DoD Instruction 4630.8, CJCS Instruction 6212.01, CJCS Instruction 3170.01, and the JCIDS Manual to

ensure information supportability is addressed in the Information Support Plan (ISP) and Capabilities Production Document.
- Submit the ISP for formal, coordinated, Final ISP of Record Review according to DoD Instruction 4630.8 and Pilot Memorandum, OASD(NII), "Information Support Plan (ISP) Acquisition Streamlining Pilot Program," August 26, 2005 (Available to users in the ".Mil" domain at the JCPAT-E site under "ASD (NII)/DoD CIO ISP Pilot Memo and Special Interest List.").

7.3.6.2.5. After Milestone C (after Final Build Approval for Space Programs)

- Submit an updated Information Support Plan (ISP) for each major upgrade (e.g., block or increment).
- Submit the Updated ISP for formal, coordinated, Initial ISP Review according to DoD Instruction 4630.8 and Pilot Memorandum, OASD(NII), "Information Support Plan (ISP) Acquisition Streamlining Pilot Program," August 26, 2005. (Available to users in the ".Mil" domain at the JCPAT-E site under "ASD (NII)/DoD CIO ISP Pilot Memo and Special Interest List.")

7.3.6.2.6. Interoperability Test Certification

Interoperability Test Certification by Joint Interoperability Test Command will not occur without an Information Support Plan. Exceptions must be approved by both the Office of the Assistant Secretary of Defense for Networks and Information Integration, Deputy Chief Information Officer and Joint Staff J-6.

7.3.6.2.7. Family-of-Systems Information Support Plan (ISP)

ISPs for families-of-systems or systems-of-systems (i.e., portfolios, enterprises, capability areas, and similar groupings) are encouraged as a way to save time and resources. However, this ISP approach requires permission from the office of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (OASD(NII)/DoD CIO) and the Joint Staff J-6. The request should define the scope, details and expected process with OASD(NII)/DoD CIO before the family-of-systems or system-of-systems ISP is initiated. Often the systems within a particular set of systems are out of sync with programmatic acquisition events, particularly in time sequence. Frequently, this situation can be accommodated by creating a "parent" overarching, capstone, portfolio, or enterprise ISP, and adding annexes to the ISP to cover the additional systems. Each time an annex or individual element of the family-of-systems or system-of-systems is addressed, particular care should be taken to include the interactions between the elements making up the overall family- or system-of-systems and the parent operational architecture. The ISP should address information sharing and/or collaboration.

7.3.6.3. Estimated Information Support Plan (ISP) Preparation Lead Time

Based on past experience, a small program with few interfaces takes about 6 months to get an ISP ready for review. For most programs, however, ISP preparation for initial review takes about 1 year. Very complex programs, like a major combatant ship, it can take from 18 to 24 months. The length of the process primarily depends on whether an integrated solution architecture exists or requires development.

7.3.6.4. OSD Review

The Office of the Assistant Secretary of Defense, Networks and Information Integration (OASD(NII)) reviews all Information Support Plan (ISP) documents for Acquisition Category I and IA programs, and for other programs in which OASD(NII) has indicated a special interest. This review is performed on the Command, Control, Communication, Computers, and Intelligence Support Plan Assessment Tool in the Joint C4I Program Assessment Tool (JCPAT) suite. The JCPAT suite provides paperless, web-based support for ISP document submission, assessor review and comment submission, collaborative workspace, and consolidated review comment rollup. The Defense Information Systems Agency JCPAT functional analyst is available to assist users with JCPAT functionality and to establish user accounts. As a best practice, the JCPAT includes an ISP repository available for viewing archived and current ISPs.

7.3.6.5. Example/Sample Web Links

Program Managers and other stakeholders will find the links in Table 7.3.6.5.T1 useful for Information Support Plan preparation, program analysis, and oversight.

▪ **Web Site**	
NIPRNET	**SIPRNET**
▪ Defense Information Systems Agency's Joint C4I Program Assessment Tool	
https://jcpat.csd.disa.mil/JCPAT	jcpat.ncr.disa.smil.mil
▪ Defense Architecture Repository	
https://disronline.disa.mil/a/DISR/consent https://dars1.army.mil/IER/index.jsp	Not applicable
▪ Global Information Grid (GIG) Technical Direction and GIG Enterprise Service Profiles	
http://www.dtic.mil/cjcs_directives/cdata/unlimit/6212_01.pdf	Not applicable

Table 7.3.6.5.T1. Example/Sample Web Links

7.3.6.6. Points of Contacts

Useful points of contact appear in Table 7.3.6.6.T1.

Mission Areas	Phone
Land, Space, Intelligence	703-607-0246
Air, Precision Guided Munitions, Command and Control	703-607-0562
Maritime, Missile Defense	703-607-0563
Business Systems, Information Tech Systems	703-607-0490
Joint C4I Program Assessment Tool Functional Analyst	703-681-2703

Table 7.3.6.6.T1. Useful Points of Contact

7.3.6.7. Traditional Information Support Plan (ISP) (Document) Content

7.3.6.7.1. Chapter 1. Introduction

Summarize the program's relationships to relevant Joint Operating Concepts (JOCs) and/or Joint Functional Concepts (JFCs) (e.g., focused logistics), as described in the program's Joint Capabilities Integration and Development System (JCIDS) documents. Provide an OV-1 (High-Level Operational Concept Graphic) for the basic program and descriptive text. For programs not covered by JCIDS, analogous documentation may be used.

- Summarize the program's relationship to other programs.
    - Provide a graphic that shows the major elements/subsystems that make up the system being acquired, and how they fit together. (Provide an Internal SV-1 (System Interface Description)/(e.g., a system block diagram)). Identify the Joint Capability Areas down to three tiers. Use OV-2s in sufficient detail to show each associated area.
    - Analyze threat-specific information that will play a role in capability development, design, testing and operation. This information should be obtained

from the appropriate JCIDS documents. Information Operations (IO) threats should be analyzed using the Information Operations Capstone Threat Capabilities Assessment, DI-1577-12-03, August 2003. This is the most comprehensive source available for IO-related threat information.
    - For a weapon system, briefly describe the purpose, design objectives, warhead characteristics, sensors, guidance and control concept (as appropriate), command and control environment, general performance envelope, and primary Information Technology (IT), including National Security Systems (NSS), interfaces.
    - For a command and control system, describe the system's function, dependencies and interfaces with other IT (including NSS) systems.
    - For an Automated Information System (AIS), describe the system's function, its mission criticality/essentiality, dependencies, interfaces with other IT (including NSS) systems and primary databases supported.
- Provide the following program data to help the reviewer understand the level of detail to be expected in the ISP:
    - Program contact information (Program Manager, address, telephone, email address, and ISP point of contact).
    - Program acquisition category: Acquisition Category.
    - List Milestone Decision Authority: Defense Acquisition Board, Defense Space Acquisition Board, Information Technology Acquisition Board (or component Milestone Decision Authority) or other.
    - Milestone covered by the specific ISP.
    - Projected milestone date.
    - Universal Identifier/DoD IT Portfolio Repository number.
    - Document Type.

7.3.6.7.2. Chapter 2. Analysis

In analyzing a program's information needs and dependencies, the analysis must be considered in the context of the process that is critical to the capability being completed by the system. Look at the critical mission threads associated with the program and compare the operational architecture views to the system architecture views to make sure all information needs and dependencies that are critical to the capability being developed are met. Use in the integrated architectures and consider the following in the analysis:

- Analysis of the qualitative and quantitative sufficiency of Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) support (e.g., hardware, software, processes, etc.) should be accomplished in terms of the operational/functional capabilities that are being enabled.
- An understanding of the operational/functional capabilities and the metrics that define whether they are being performed adequately.
- An understanding of what enabling functional capabilities must be performed in order to achieve a higher-level capability (C4ISR functions will almost always be enabling capabilities).

- An understanding of which players (nodes) will direct or perform the missions associated with delivering the capabilities.
- An understanding of DoD Information Policies.
- A definition of the Time Phase in which the analysis is to be accomplished. A user identifies the Time Phase, or Time Phases, their program operates within and defines the Time Phase Name (i.e., increment, block, spiral, et al.), Year, and a Description.
- The information-needs discovery process. For most systems, the steps that follow this list provide an information-needs discovery process that can be used to analyze the system under development. Other approaches for discovering information needs that apply to the intelligence information needs discovery process are:
    - Using the stages of the intelligence cycle (collection, exploitation, dissemination, etc.).
    - Life-cycle stages (Concept Refinement, Technology Development, System Development and Demonstration, etc.).
- The following steps (and notes) are based on using the Integrated Architecture developed in accordance with the DoD Architectural Framework, during the JCIDS process.

Step 1: Identify the warfighting missions and/or business functions within the enterprise business domains that will be accomplished/enabled by the system being procured.

The Mission Threads are based on the last version of the Joint Capability Areas and allow a developer to bin a program's capabilities. A developer selects a Tier 1 Mission Thread in the Enhanced ISP and is then able to select the Tier 2 and Tier 3 mission threads that are children of the chosen Tier 1.

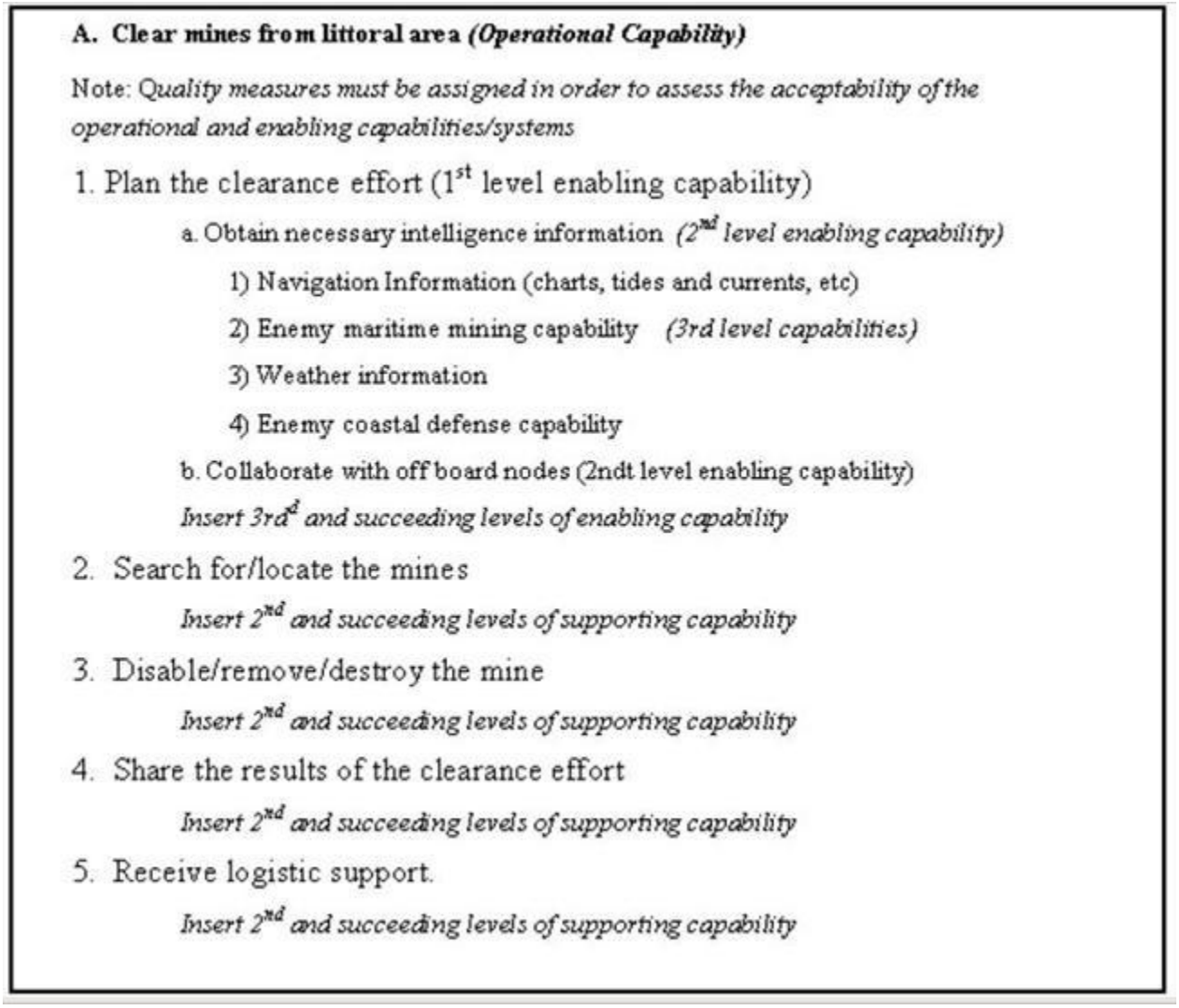
Note: Joint Capability Areas are found at: http://www.dtic.mil/futurejointwarfare/cap_areas.htm

Step 2: Identify information needed to enable operational/functional capabilities for each warfighting mission identified in Step 1 by performing functional capability decomposition.

Note: If a Command and Control capability is the top-level driver of the function breakdown, then the OV-4 (Command Relationships) will be a necessary product to help define the functional capabilities needed. The OV-4 will likely require several OV-5 (Activity Model) functional breakdowns to enable each of the command elements identified.

Note: The architecture product most useful in managing the discovery of enabling/enabled capability relationships for each operational/functional capability is the OV-5 (Operational Activity Model). The OV-5 can be used to show the subordinate capabilities that are necessary to achieve a higher-level operational or functional capability. Notice that the OV-5 focuses on "what" rather than "how." See Example Capability Breakdown, Figure 7.3.6.7.2.F1. This example illustrates specific items to consider for a weapon system that can be used to get the flavor of what is expected in step 2 for a program/system.

Step 2 Example: Clear Mines from Littoral Area



A. Clear mines from littoral area *(Operational Capability)*

Note: *Quality measures must be assigned in order to assess the acceptability of the operational and enabling capabilities/systems*

1. Plan the clearance effort (1st level enabling capability)
    a. Obtain necessary intelligence information *(2nd level enabling capability)*
        1) Navigation Information (charts, tides and currents, etc)
        2) Enemy maritime mining capability *(3rd level capabilities)*
        3) Weather information
        4) Enemy coastal defense capability
    b. Collaborate with off board nodes (2ndt level enabling capability)
    Insert 3rd and succeeding levels of enabling capability
2. Search for/locate the mines
    Insert 2nd and succeeding levels of supporting capability
3. Disable/remove/destroy the mine
    Insert 2nd and succeeding levels of supporting capability
4. Share the results of the clearance effort
    Insert 2nd and succeeding levels of supporting capability
5. Receive logistic support.
    Insert 2nd and succeeding levels of supporting capability

Figure 7.3.6.7.2.F1. Example Capability Breakdown

Note: The specific form of this information should capture key information from an OV-5 (Operational Activity Model) and/or other information source (e.g., an outline or hierarchical graph). The important point is that the capability relationships are understood and attributes are identified so that assessments can be made.

Note: Specific items to consider:

- For satellite systems include: (e.g. Satellite control).
- For communication systems include: (e.g. Net-management).
- For business process systems include: (e.g. information contained in databases, other information sources).

- For weapons systems include: (e.g. Collection Management Support, Threat or signature support, targeting support, Intelligence Preparation of the Battlefield).
- For sensor systems include: (e.g. Collection Management support, Threat or Signature support, Targeting support, Intelligence Preparation of the Battlefield, and Remote Operations).
- For platforms consisting of a mix of the above include: (e.g., Collection Management support, Threat or Signature support, Targeting support, Intelligence Preparation of the Battlefield.

Step 3: Determine the operational users and notional suppliers of the information needed.

Step 3.a: Provide an OV-2 to identify the operational nodes and elements that drive the communications needed to enable the functional capabilities. For large platforms/systems, this effort should identify the major operational nodes (information drivers) within the platform, as well as nodes that are external to the platform/system with which information will be shared.

Step 3a Example: Clear Mines from Littoral Area

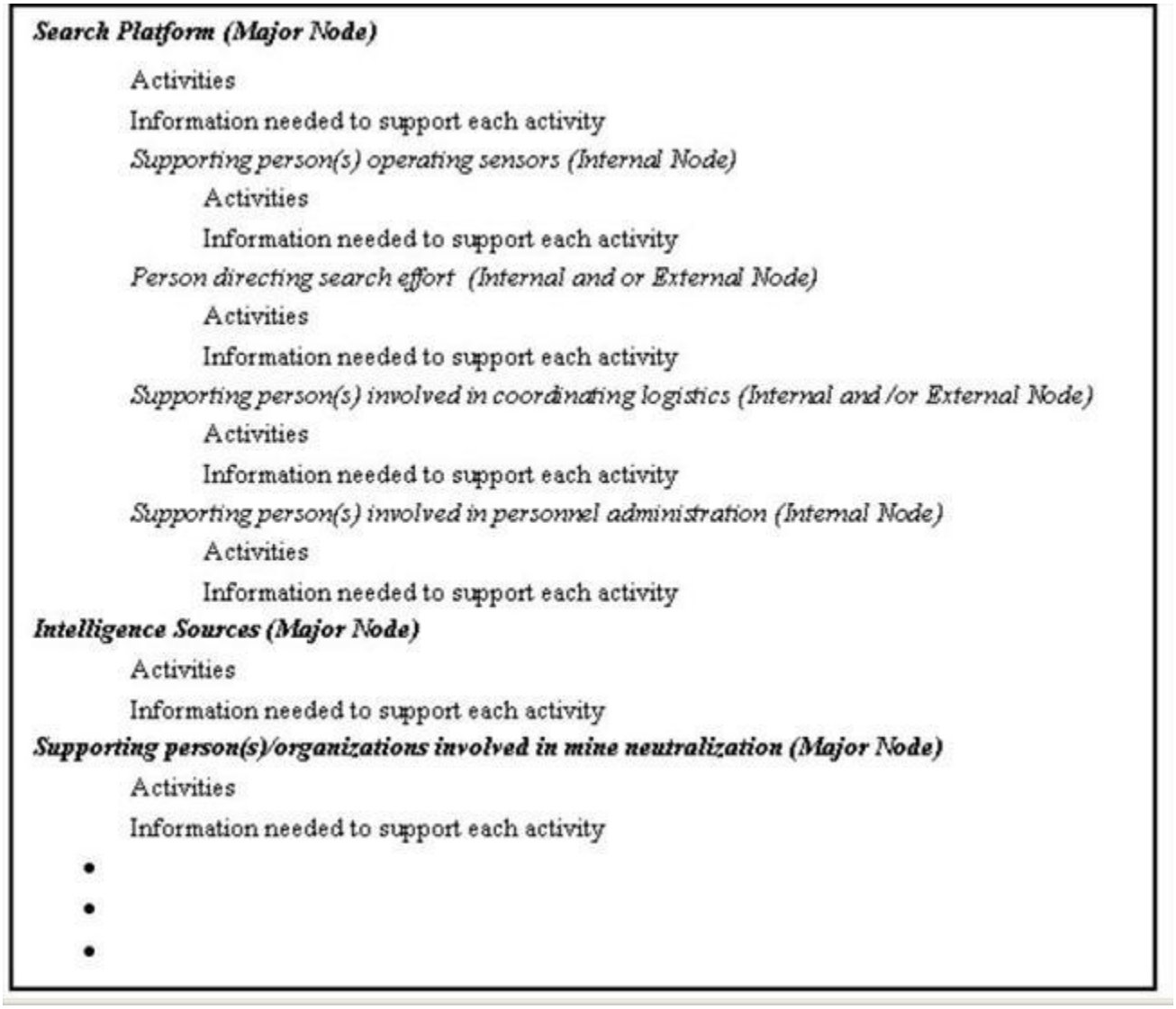


Figure 7.3.6.7.2.F2. Example OV-2 Nodes for Mine Clearance

Step 3.b: Map these nodes (internal and external systems and people) and their activities to the functions identified in OV-5.

Step 4: Establish the quality of the data needed to enable the functions identified in OV-5 and performed by the operational nodes in OV-2 (Operational Node Connectivity).

Note: Establish performance measures and determine the level of satisfaction necessary to make the information useful. (Examples: decimal precision for numerical data, NIIRS for imagery, annotated versus raw data, etc.)

Note: When radio and other information transport systems are identified as providing support, establish transmission quality parameters and then assess whether the programs/systems intended to be used can meet these criteria.

Note: A factor in determining quality is the user (person or sub-system) (i.e., specifically how does the user intend to use the information).

Step 5: Determine if timeliness criteria exist for the information.

Note: To help establish timeliness, use OV-6C (Operational Event Trace Diagram) to establish event sequence. Considerations include:

- Order of arrival of information to enable transaction process(es) (for weapon systems) Latency of data due to speed of flight issues.
- Currency of data in databases to support operations.

Step 6: Determine/Estimate the quantity of information of each type that is needed.

Factors influencing quantity include:

- Frequency of request or transmittal.
- Size of the information requested (packet size, image size, file size etc.).
- Whether data is individual items or a data stream that is provided for a period of time.
- Whether data transmission is "bursty" or continuous over some period of time.
- Whether data transmission is random or occurs at some predictable interval.
- The anticipated spectrum of employment (e.g. Military Operations Other than War or Major Theater of War).

Note: Ultimately this analysis should help estimate the bandwidth needs and should provide an assessment as to whether adequate bandwidth is available. If bandwidth is limited, what actions can be taken to reduce demand or use the bandwidth more efficiently?

Step 7: Discuss the way information will be accessed or discovered.

If data links are involved, identify them and also the message sets that will be implemented.

If an Internet/Web-based (Global Information Grid (GIG) compliant) means of searching for and retrieving posted data is to be used, describe the approach, including compliance with DoD Instruction 8410.01, "Internet Domain Name Use and Approval."

- Data stores must exist for your program.
- The type of searching capability needed.

Note: In many cases, this discussion will involve multiple levels of enabling systems. For example, maybe the enabling system is a Global Command and Control System (GCCS) application. GCCS rides on the Secret Internet Protocol Router Network (SIPRNET). So both levels of this support should be discussed.

Step 8: Assess the ability of supporting systems to supply the necessary information.

Identify the external connections to the system using the system views and identify any synchronization issues associated with schedule and/or availability of external systems.

Note: Supporting systems include collection platforms, databases, real time reports, messages, networked data repositories, annotated imagery, etc.

- Assess the ability to collect, store, and tag (to enable discovery and retrieval) the information.
- Assess the ability of networks to provide a means to find and retrieve the necessary data.
- Assess the ability of the information transport systems to move the volume of data needed.
- Assess synchronization in time (i.e., years relative to other system milestones) with supporting programs.
- Whether the information will cross security domains.

Note: If systems will in any way tie into the intelligence Top Secret (TS)/ Sensitive Compartmented Information (SCI) network, Joint Worldwide Intelligence Communications System, or utilize TS/SCI information, they will have to comply with Director, Central Intelligence Directives (DCID): DCID 6/3, "Protecting Sensitive Compartmented Information within Information Systems," June 1999 and DCID 6/9, "Physical Security Standards for Sensitive Compartmented Information Facilities," 18 November 2002.

Note: The number of levels of analysis will depend on the detail required to identify the critical characteristics of the information needed to support the program. This should be accomplished for all phases of the acquisition life cycle.

Note: It is anticipated that the other communities such as the intelligence community may have to assist in the determination and analysis of these information needs.

Step 9: Assess Radio Frequency (RF) Spectrum needs.

Note: DoD Instruction 4650.01 establishes spectrum management policy within the Department of Defense. (DoD Instruction 4630.8 and CJCS Instruction 6212.01 require Spectrum Supportability (e.g., spectrum certification, reasonable assurance of the availability of operational frequencies, and consideration of Electromagnetic Environmental Effects) to be addressed in the ISP. The Services have additional spectrum management policies and procedures.

To support the Spectrum Supportability process, the ISP should document the following:

- Requirements for use of the electromagnetic spectrum including requirements for wide bandwidths.
- Description of the intended operational Electromagnetic Environment (Allows for realistic test and evaluation).
- Impact of the loss of a planned spectrum-dependent command, control, or communication link as a result of an unresolved spectrum supportability issue. (To be identified in the issue section of the ISP.)

Note: For platforms that employ RF emitters developed by a separate acquisition program, spectrum documentation for those emitters may be cited here as evidence of compliance with Spectrum Supportability regulations.

Step 10. Assess Net-Centricity.

Note: Consider individual Services net-centric policies and procedures that supplement DoD Net-centric policy.

Note: This is an emerging requirement in the analysis required for ISPs. When Net-Centric Enterprise Services (NCES)/Core Enterprise Services (CES) is available, programs will be expected to conduct this as a detailed analysis. Programs should be aware of this developing requirement, as it will become an essential part of determining net-centricity and compliance with the DoD Information Enterprise (IE).

Step 10a: Using the information provided as a result of Step 7, the PM should evaluate the program against measurement criteria from the DoD Information Enterprise Architecture (IEA) V1.1.

Step 10b: Provide an analysis of compliance with the emerging Net-Centric Enterprise Services (NCES)/Core Enterprise Services (CES).

As the DoD IE CES develops, its specifications should be cross-walked with the ISP system's planned network service specifications. Identify the issues associated between the CES service specifications and those of the system that is the subject of the ISP. Compliance would mean that the system would connect seamlessly with the defined DoD-level enterprise services.

Step 10c: Assess use of the following:

- Software Compliant Radios (Joint Tactical Radio System)
- Internet Protocol Version 6.0
- DoD Net-Centric Data Management Strategy
- GIG Bandwidth Expansion relationships
- Net-Centric Enterprise Services linkages

Step 11: Discuss the program's inconsistencies with the DoD Enterprise Architecture and the program's strategy for getting into alignment.

Identify areas where the latest versions of the DoD Architecture Framework (DoDAF) and DoD Information Enterprise Architecture (IEA) V1.1 do not support information needs. (See also DoD Directive 8000.01.)

Step 12: Discuss the program's Information Assurance (IA) strategy. Also provide a reference to the Program Protection Plan, if applicable.

Step 13: Identify information support needs to enable development, testing, and training.

For development: Weapon systems include information about potential targets that are necessary to support system development. (Example: target signature data)

For testing: Include information support needs critical to testing (Example: Joint Distributed Engineering Plant (JDEP)). Do not duplicate Test and Evaluation Master Plan information except as needed to clarify the analysis. In addition, for information on software safety testing please refer to section 9.3.1.

For training: Include trainers and simulators that are not a part of the program being developed. Include:

- Separately funded training facilities your program intends to use.
- Network support that will be needed to meet the training needs of your program.

7.3.6.7.3. Chapter 3. Issues

- Identify risks and issues (as defined in DoD Instruction 4630.8) in a table similar to Table 7.3.6.7.3.T1 or in an outline containing the same data.
    - Group operational risks and issues under the mission impacted, then under the impacted functional capability (for that mission).
    - When risks or issues involve more than one mission, subsequent missions should be marked with the previous issue number and those fields that remain the same should be so marked.
- Include the following column (or outline) headings:
    - Issue Number
    - Supporting System
    - Source Integrated Architectures (e.g., Command and Control (C2), Focused Logistics, Force Protection, Force Application, Battlespace Awareness, Space, etc.)
    - Issue Description
    - Risk/Issue Impact (Use the AT&L "Risk Management Guide for DoD Acquisition" for this assessment)

- Mitigation Strategy or Resolution Path

Operational Issues					
Mission					
Functional Capabilities Impacted					
Issue Number	Supporting System	Source Architecture	Issue Description	Issue Impact	Mitigation Strategy/ Resolution Path (and Time-Frame)
Development Issues					
Testing Issues					
Training Issues					

Table 7.3.6.7.3.T1. Sample Issue Table Format

Risks and issues considered critical to the program's success will be briefed by the Program Manager (PM) at Overarching Integrated Product Team meetings. At a minimum, information risks and issues will be incorporated into the PM's risk management program and treated as any other type of program risk and issue.

7.3.6.7.4. Information Support Plan (ISP) Appendices

Appendix A. References. Include all references used in developing the ISP. Include Architectures; other relevant program documentation; relevant DoD, Joint Staff, and Service Directives, Instructions, and Memos; ISPs or ISPs from other programs; any applicable Joint Capabilities Integration and Development System documentation; and others as deemed necessary.

Appendix B. Systems Data Exchange Matrix (SV-6).

Appendix C. Interface Control Agreements. Identify documentation that indicates agreements made (and those required) between the subject program and those programs necessary for information support. For example, if System A is relying on information from System B, then this interface dependency must be documented. At a minimum, this dependency should be identified in the ISPs for both System A (the information recipient) and System B (the information provider).

Appendix D. Acronym List: Provide an Integrated Dictionary (AV-2).

Other Appendices. Provide supporting information, as required, not included in the body of the ISP or relevant Joint Capabilities Integration and Development System documents. Additional or more detailed information used to satisfy DoD Component-specific requirements should be included as an appendix and not incorporated in the body of the subject ISP. Additional

architecture views used in the ISP analysis will be provided in a separate appendix and referenced in the main body of the ISP.

7.3.6.8. Enhanced Information Support Plan (EISP) Instructions

7.3.6.8.1. Description

The EISP allows Program Managers (PMs) to create an Information Support Plan (ISP) or Tailored Information Support Plan (TISP) using the EISP tool (both EISP and TISP using EISP are here after referred to as the EISP) through an improved process that focuses on the information elements that are most important to successful implementation for the warfighter. This new process transitions the ISP from a document-centric to a data-centric process. The goal is to save time and resources while retaining the value of an ISP. The EISP is "data-centric" vice "document-centric". It focuses on the analysis of a program's processes (operational activities performed to complete a mission), and critical information needs and their dependencies (data and information passed between operational nodes via system implementations that enable mission completion). Using the EISP tool, PMs will be able to enter their ISP data through formatted templates that provide two different types of functionality:

- Structured input—TurboTax®-like—that prompts users to enter specific required information in specific places.
- Flexible arrangement—Lego® block-like—that allows users to enter additional data and information relevant to their particular program that may not be required by the structured sections, but is necessary for understanding the program.

The data entered into the EISP tool will be tagged with Extensible Markup Language (XML). XML tagging is transparent to the user and requires no PM actions. It enables the data to be easily stored, searched, retrieved, and reused. The EISP standardizes the format of an ISP, but the content as defined in DoD Instruction 4630.8 and here in, remains mostly unchanged. The EISP includes a methodology for outputting the data in Portable Document Format, eliminating the need for PMs to spend time formatting and producing an ISP or TISP document.

7.3.6.8.2. Use of Enhanced Information Support Plan (EISP) Tool

Since October 2008, Program Managers (PMs) are encouraged to use the EISP tool for all new-start initial Information Support Plans (ISPs). PMs who have already started an ISP may transition to the EISP if they so choose. The goal is to have all new ISPs created with the EISP tool no later than Fiscal Year 2010. The EISP process is illustrated in Figure 7.3.6.8.2.F1 below. The ISP developer downloads or requests a copy of the EISP from Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer. An updated EISP Guidebook will be provided with the EISP tool. The EISP utilizes Extensible Markup Language (XML) to tag program and architecture data through the use of formatted templates that guide the entry of information. As information is entered into these templates, an XML file and an XML metacard are produced. The XML file can be automatically converted into Portable Document Format for review. The XML file will become the basis for making the ISP data available to the DoD and other stakeholders. The XML file can be reused for other analytical processes as well as exported to support other data calls. The XML metacard allows discovery of ISP keyword data online. The metacard contains ISP PM contact information, for users to request permission to view the full ISP. All or part of the ISP XML file can be reused in the creation of new ISPs.

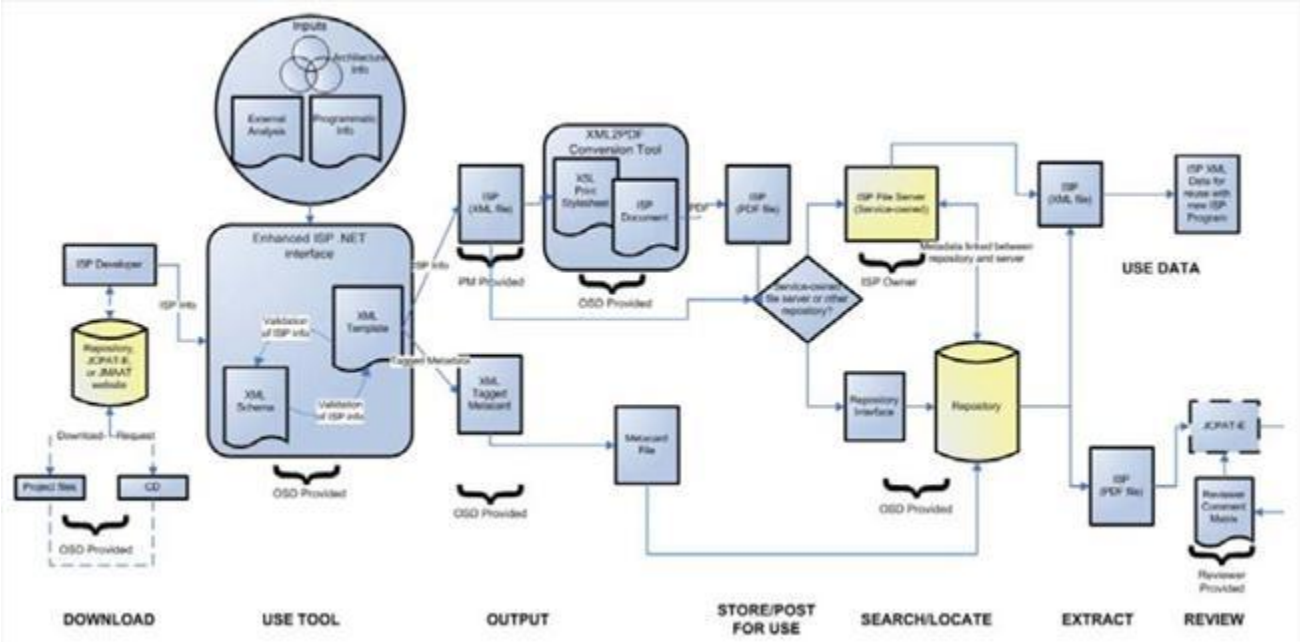


Figure 7.3.6.8.2.F1. Enhanced ISP Process

7.3.6.8.3. Enhanced Information Support Plan (EISP) Sections

The EISP is divided into sections that fulfill the requirements of DoD Instruction 4630.8 "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)."

Section 1. Introduction

Section 1.1. Program Information

The first section of the EISP is the Program Information section. These forms are inputs for basic information about a program, including:

- Program Name
- UID/DITPR number
- Document Type
- ISP Release/Revision Date
- ISP Draft Status
- ISP Classification, including:
- Caveats
- Overall ISP Classification
- ISP Classified by
- ISP Classification Derived from
- ISP Declassify On
- Program Logo
- ISP Version
- ISP Document Control Number
- ISP Milestone
- Distribution Statement

In the EISP output, this information is used to build the Information Support Plan (ISP) Portable Document Format (PDF) cover sheet. If the developer chooses to create a classified ISP they are warned that they must be working in a secure environment to continue. Once the developer has chosen to create a classified ISP they will have the ability to add classification markings, including caveats, to the EISP. Paragraph markings will appear for all text sections and the ability to mark tables and graphics will become active. The overall classification of the EISP output will be defined based on the highest classification level used in the paragraph and graphics markings.

Section 1.2. Program Data

The Program Data sections of the EISP request additional information about the program.

Signature Page. The Signature Page allows users to add signature lines to the second page of the EISP output. Users may enter as many signature lines as are necessary for their program. A signature line requires a:

- Name
- Rank
- Title

The EISP output will display a line for a signature and a line for a date above this data.

PM Contact Information. The Program Manager (PM) Contact Information allows a PM to enter their contact information. Contact information is only required for one PM for each program. Additional contact information should be added to the ISP Point of Contact section.

ISP Point of Contact. The ISP Point of Contact section allows for the addition of contact information other than the PM. The information requested in this section is the same as the PM Contact Information section. The user has the ability to enter information for more than one person.

Program Acquisition Category. The Program Acquisition Category contains fields for denoting the acquisition category the program falls under, and whether or not the program is a special interest program.

ISP Approval Authority. This section allows a PM to identify the approval authority.

Projected Milestones. The Projected Milestones section has user fields to enter information about the program's schedule and milestones. The user is able to include:

- Projected Milestone Date
- Program Schedule File
- Program Schedule Graphics
- Program Schedule Text

The user may choose the file type for the Program Schedule File. This file has to be submitted along with the EISP output for review; the EISP does not automatically bundle Program Schedule Files in the output. On the other hand, the Program Schedule Graphics may be any graphics file; it will be displayed in the EISP output.

Communities of Interest. The Communities of Interest section allows a user to identify the relevant communities of interest. It contains the following fields:

- Community Name
- Community Type
- Community Description

A user can input as many Communities of Interest for their program as necessary.

Supporting Documentation. The user should identify detailed, supporting documentation in this section.

Section 1.3. Overview

Introduction. The Introduction allows a user to enter free text to introduce a reviewer to their program. A user can enter text into the introduction table and each new row of text in the table will be created as a new paragraph in the EISP output. The Introduction also contains a Supporting Documentation section allowing the user to attach relevant graphics or notes.

Acquisition Oversight Authority. The Acquisition Oversight Authority section contains fields to collect data pertaining to the program's appropriate Acquisition Board. A user can choose from the following boards and complete the data fields under each board:

- Defense Acquisition Board
- System Name
- Purpose
- Design Objectives
- Warhead Characteristics
- Guidance and Control Concepts
- Command and Control
- Primary Information Technology
- Information Technology Board
- System Name
- System Functions
- Management Functions
- Control Functions
- Defense Space Acquisition Board
- System Name
- System Functions
- Management Functions
- Control Functions
- Special Defense Acquisition Board (Intelligence)
- System Name
- System Functions
- Management Functions
- Control Functions
- Database
- Component Acquisition Board
- Component
- System Name
- Purpose
- Design Objectives
- Warhead Characteristics

- Guidance and Control Concepts
- Command and Control
- Primary Information Technology

A user may provide data for multiple acquisition boards, but only the board selected in the tool will display in the output.

Supporting Documentation. The user should identify detailed, supporting documentation in this section.

Section 2. Analysis

The Analysis section of the EISP contains most of the information found in the second chapter of a traditional ISP. It is where a large part of the data collection to create the EISP is completed.

Process Analysis. The Process Analysis section is the most important section of the EISP Analysis. This section is structured hierarchically; each level of the hierarchy, and how deep the hierarchy goes, is defined by the user. The final outputs of the Process Analysis section are risks and issues for the program. Once the Process Analysis section is complete the user will have a base of operational risk and issues to work with.

The first level of the Process Analysis hierarchy is Time Phase. The user identifies the Time Phase or Phases, within which the program operates and defines the:

- Time Phase Name
- Year
- Description

Each Time Phase decomposes into Operational Nodes and Mission Threads. Operational Nodes allow a user to enter data defining all the nodes, internal and external, that interact with their program. Operational nodes are derived from a program's OV-2 or, once completed, node information can be used to develop an OV-2. An OV-2 can be attached, as a graphic, to operational nodes. A developer completes the Operational Node section by filling out:

- Node Name
- Node Number
- Internal/External
- Node Description
- Node Type
- Node Graphics

An Operational Node can be broken down into its sub-operational nodes. Operational nodes are later referenced as either producers or consumers of an information need. At the lowest sub-operational node level, a developer has the ability to define which System Nodes are utilized by

the Operational Node. System nodes are derived from a program's SV-2 or, once completed, node information can be used to develop an SV-2. A developer completes the System Node section by filling out:

- Node Name
- Node Number
- Internal/External
- Applicable KIPS/NCIDS
- Node Description
- Radio Frequency (RF) Emitter (yes/no)
- Datalink (yes/no)
- Message Sets

Any system node marked as an RF Emitter will appear in the RF Spectrum Needs section of the EISP and a developer will have to provide additional RF information for the system. System nodes can be referenced as either producers or consumers of a system implementation.

Once all the nodes that interact with a program are entered, a developer will begin to define the Mission Threads within which that program operates. The Mission Threads in the EISP are based on the last version of the Joint Capability Areas and allow a developer to bin a program's capabilities. A developer selects a Tier 1 Mission Thread in the EISP and is then able to select the Tier 2 and Tier 3 mission threads that are children of the chosen Tier 1.

Once Mission Threads are defined, a developer will define the Activities the program performs. Activities are derived from a program's OV-5 or, once completed, this information can be used to develop an OV-5. An activity's OV-5 can be attached as a graphic in this section. A developer completes an activity by populating the following fields:

- Task List Name
- Activity Number
- Activity Name
- Activity Description
- Activity Start Time
- Activity Duration
- Keywords
- Activity Graphics

Activities can be broken down into the sub-activities that comprise them. At the leaf activity level, a developer defines the "Information Needs" required to complete the parent activity. Information needs reference operational nodes, as the operational nodes previously defined are options in the information need forms. To complete an Information Need, a developer populates the following fields:

- Information Need Name

- Information Need Source
- Information Need Consumer
- Information Need Identifier
- Information Need Type
- Information Need Description

The developer then answers yes or no to a series of questions, displayed as checkboxes in the EISP, to determine the depth of the required, remaining analysis. If a developer checks any of these options, they are required to provide further analysis related to their program:

- Is this Information Need critical or external to the program?
- Is this Intelligence Supportability Related?
- Are there Minimum Parameters for this information?
    - Quality
    - Quantity
    - Timeliness

If a developer determines that minimum parameters do exist, they must define the metrics of those parameters. This information will lead to further analysis in the EISP. Any checks in these boxes will require the developer to continue on to the System Implementation section of the EISP. System implementations reference system nodes, as the system nodes previously defined are options in the system implementation forms. To complete a System Implementation a developer completes the following:

- System Implementation Name
- System Implementation Source
- System Implementation Consumer
- Transport Methodology
- Data Sharing Characteristics

The Data Sharing Characteristics only become active if "TCP/IP" is selected as the Transport Methodology. A developer is then able to define the data sharing characteristics of a system implementation by checking the following characteristics that apply:

- Tagged
- Discoverable
- DoD Metadata Registry/DoD Discovery Metadata Standard Registered
- Internet Protocol Version 6 Capable
- Web Service

If a developer has defined minimum parameters previously, they will be asked if this system implementation can meet these parameters. If the systems meet the parameters, the analysis for this particular implementation is complete. If the systems do not meet the parameters, the developer will be required to create a risk or issue explaining why the parameter cannot be met.

Risks and Issues, as defined by the "Risk Management Guide for DoD Acquisition," are differentiated by whether or not their root cause has already occurred. If a developer states a parameter is not met and that this root cause has not already occurred they must complete a Risk in the EISP. The Risk template is defined by the "Risk Management Guide for DoD Acquisition" and contains the following fields:

- Risk ID
- Risk Name
- Impacted Activity
- Source of Risk
- Risk Type
- Risk Level
- Risk Impact
- Mitigation Strategy
- Future Root Cause

Risk ID and Impacted Activity are determined by the EISP with Risk ID being generated based on the number of other risks in the ISP and Impacted Activity being the parent activity of the risk. The Risk Level is calculated base on the developers choices for the likelihood and consequence of the risk based on the Risk Management risk cube. All risks generated in Process Analysis will be displayed in chapter 3 of the output and will link to the system implementation that generated it in chapter 2 so a reviewer can see the risk in context of the process analysis hierarchy.

If a developer states a parameter is not met and that this root cause has already occurred they must complete an Issue in the EISP. The Issue template is defined by the "Risk Management Guide for DoD Acquisition" and contains the following fields:

- Issue ID
- Issue Name
- Impacted Activity
- Source of Issue
- Issue Type
- Issue Level
- Issue Description
- Issue Impact
- Mitigation Strategy

Issue ID and Impacted Activity are determined by the EISP with Issue ID being generated based on the number of other issues in the ISP and Impacted Activity being the parent activity of the issue. The Issue Level is calculated base on the developers choices for the consequence of the issue based on the Risk Management risk cube. Because the issue has already occurred, a developer is not able to choose the likelihood of the issue. All issues generated in Process Analysis will be displayed in chapter 3 of the output and will link to the system implementation

that generated it in chapter 2 so a reviewer can see the issue in context of the process analysis hierarchy.

The Net-Centricity section of the EISP contains questions regarding the Net-Ready Key Performance Parameters and the Net-Centric Design Tenets. Users must answer these questions and both the questions and the user's responses will appear in the EISP output.

The Information Assurance (IA) Strategy Status section allows a user to input data pertaining to a program's strategy for IA. This section contains the following forms:

- Program Protection Plan Reference
- Program Protection Plan Completion Date
- IA Strategy Title
- IA Strategy Location
- IA Strategy Status
- IA Strategy Completion Date

The section also contains a Point of Contact table and a Supporting Documentation section.

The Other Information Needs and Additional Operations Risks sections allows users to enter information needs and risks and issues that do not fall within the context of Process Analysis. Users are able to enter information and risks and issues for the following categories, and then will have to complete the fields listed under each category:

- Development
- Testing
- Training
- Operational

Operational risks and issues identified in this section should be overarching risks and issues that do not relate specifically to an activity within Process Analysis. All risks and issues in this section appear in chapter 3 of the output, but do not link to any additional information as the risks and issues generated in Process Analysis do. The section also contains Supporting Documentation.

This section allows users to assess the Radio Frequency (RF) spectrum needs of the program and document any associated RF risks and/or issues the program may encounter. System Nodes that are marked as RF emitters in Process Analysis will appear in the RF table and users are required to input the following:

- RF Frequency
- JF12 Status
- DD1494 Status
- DD1494 Date

Users are able to enter any associated risks and issues using the same templates that are found in Process Analysis. These RF risks and issues will be displayed in chapter 3 of the EISP output. The section also contains Supporting Documentation.

The Miscellaneous Analysis section requires a user to answer questions pertaining Global Positioning System (GPS) and DoD Information Technology Portfolio Repository. A user will answer the following questions:

- Does the program include a requirement for NAVSTAR GPS and precise positioning system (PPS)? And if so:
    - Does the program clearly state that the system will develop and procure only selective availability anti-spoofing module (SAASM) based equipment?
    - Is the program in the DoD IT Portfolio Registry?
    - Does the program use web-enabled processes?

Supporting Documentation. Detailed Supporting Documentation information can be found in the Supporting Documentation section.

Section 3. Appendices

The Appendices section of the EISP allows developers to enter additional information about their program. The Appendices have fields to input references cited in the EISP that are then displayed in the output.

Developers can include the program's System Data Exchange (SV-6) and the title of the exchange will be listed in the output but the file itself must be submitted separately along with the EISP output. Developers have a table to enter interface control agreement information. The titles of these agreements will appear in the output. This section also contains fields for developers to enter an acronym list for their program which is displayed in the output.

Attachments to the EISP can be added in the Appendix also, the titles of these attachments will appear in the output but the attachments themselves must be submitted separately along with the EISP output.

The final appendix allows a developer to attach a TV-1 and TV-2 to the EISP. The titles of these attachments will appear in the output but the attachments themselves must be submitted separately along with the EISP output. A developer can also enter a TV:

- Waiver Status
- Waiver Date

The Supporting Documentation sections are found throughout the EISP. These sections allow a developer to include text, graphics, keywords, and author notes that do not fall in another section

of the EISP. Free text and graphics will appear in the EISP output in the Supporting Documentation section in which they are entered.

Keywords are not displayed in the EISP output. These keywords are included in the metacard that is generated by the EISP. These keywords are what third party users will search on to find the EISP once it is stored in a repository. Keywords entered in multiple Supporting Documentation sections will be consolidated in the metacard.

Author notes are not displayed in the EISP output. These notes allow a developer to enter free text that can be used as the developer sees fit, for example to leave a reminder to complete a section. These notes are only visible to a developer using the EISP.

7.3.6.8.4. Obtaining the Enhanced Information Support Plan (EISP)

An EISP installer, along with the EISP documentation, is available from the JCPAT-E website. In addition to the installer, an EISP Guidebook and technical users guide for the EISP can also be downloaded from the JCPAT-E website. If a user has a problem downloading or installing the EISP, they can contact eisp_help@bah.com.

7.3.6.8.5. Creating the EISP

The Enhanced Information Support Plan (EISP) process focuses on Information Support Plan (ISP) data as opposed to the ISP document. The ISP developer will no longer have to write a document that may or may not be consistent with the Defense Acquisition Guidebook. Instead, he/she will be asked to enter data into an EISP template that focuses on the core informational aspects of the program. Figure 7.3.6.8.5.F1 is a sample page from the EISP Template.

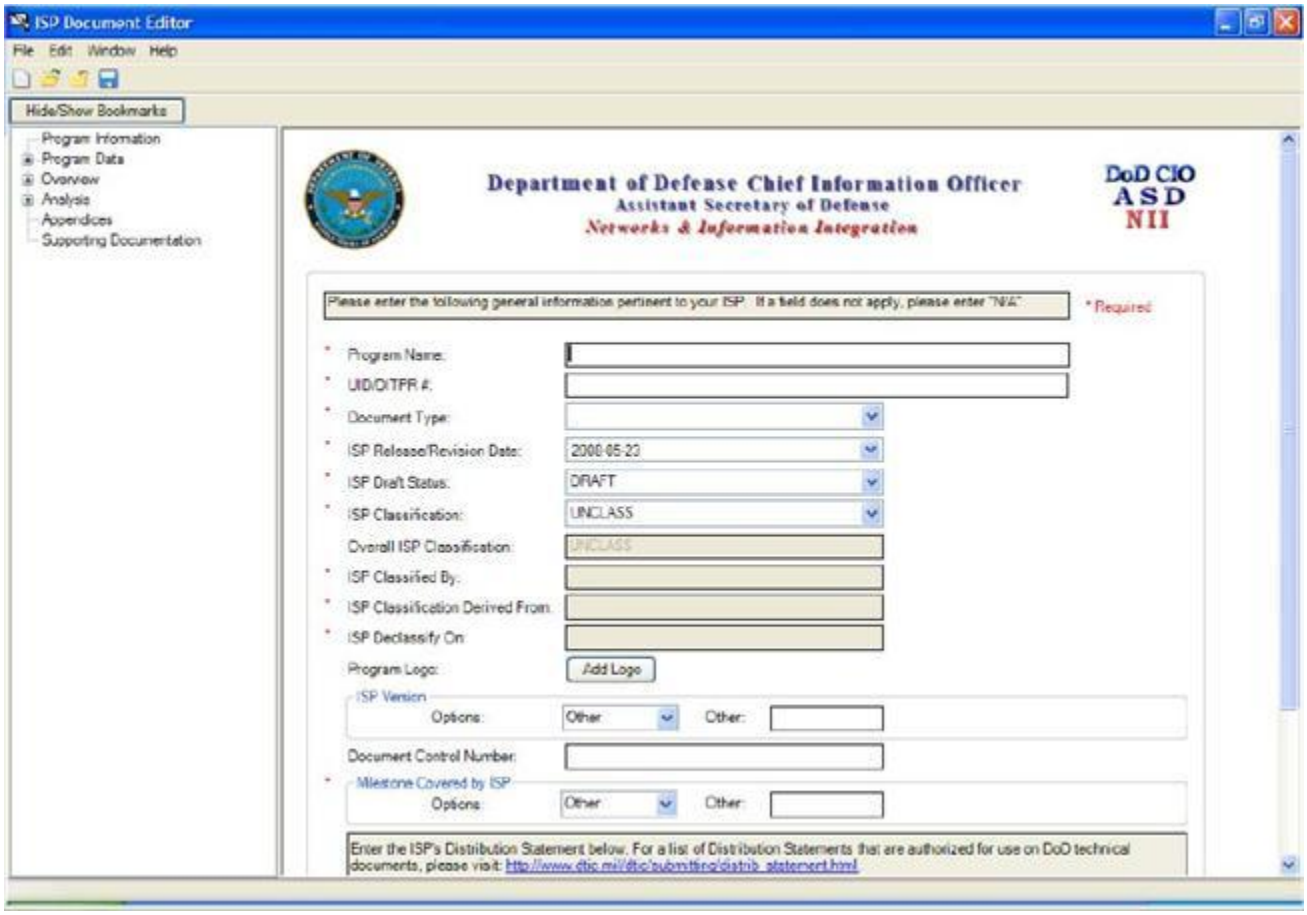


Figure 7.3.6.8.5.F1. ISP Template

Data is entered into the EISP template via the Enhanced ISP Tool. Both the tool and the system are referred to as the "EISP." The EISP is a government application that supports data entry through formatted templates. While the ISP developer enters data, the tool tags the same data in Extensible Markup Language (XML). The XML file can then be stored in a database or server (either Service or DoD owned) to enhance discoverability. The EISP also has the ability to validate data for structural correctness and completeness. For example, if the ISP developer does not enter data for a mandatory field (e.g., ISP Classification), the EISP will notify the ISP developer of the error.

7.3.6.8.6. Enhanced Information Support Plan (EISP) Reviews

7.3.6.8.6.1. DoD Chief Information Officer (CIO) EISP Review Process

Information Support Plans (ISPs) created using the EISP will be submitted to Joint C4I Program Assessment Tool - Enhanced (JCPAT-E) as a Portable Document Format (PDF) file. This PDF will be the output of the Extensible Markup Language (XML) transformation that is available with the EISP. Any additional documentation (e.g. attachments, appendices) must be submitted with the PDF, as the EISP does not include external documents when creating the output. The EISP Reviewer file explains the format of the EISP output and explains how to interpret an EISP. For detailed instructions on the ISP review process, please reference the "Information Support Plan (ISP) Acquisition Streamlining Pilot Program," August 26, 2005 (Available to users in the ".Mil" domain at the JCPAT-E site under "ASD (NII)/DoD CIO ISP Pilot Memo and Special Interest List.").

7.3.6.8.6.2. Enhanced Information Support Plan (EISP) Output for External Reviewers

For each process analyzed, there are three tables associated with it:

- Information Needs,
- Supportability Assessment, and
- Data Strategy Assessment.

The examples below analyze the "Plan Mission" Process depicted in the notional "Tables" appearing in Figures 7.3.6.8.6.2.F1 through Figures 7.3.6.8.6.2.F3

Information Needs

Information Needs

Table **2-1A** Information Needs for ***Plan Mission*** Process

Info Need #	Need Name	I/O	Producer	Consumer	Minimum Parameters: Ql | Qn | T | O	Transport Methodology
O1	***Operational area restriction***	***I***	***ON 2 – Tactical Airspace Control Authority***	***ON 1.1 – Aircraft Mission Commander***	***X / - / X / -***	-
S1.1	See Table ***2-1B***	-	SN 1.3.3.1.1 – RT-1794(C) AN/ARC-210	SN 1.3.3.1.1 – RT-1794(C) AN/ARC-210	All param met? No	Voice
O2	***Communication Plan***	***I***	***ON 2 – Tactical Airspace Control Authority***	***ON 1.1 – Aircraft Mission Commander***	- / - / - / -	-
O3	***Mine Warfare Plan***	***O***	***ON 5.1 – TSC/CDC/CIC***	***ON 1.1 – Aircraft Mission Commander***	- / - / - / -	-
S3.1	See Table ***2-1B***	-	SN 5.4 – IT-21	SN 5.4 – IT-21	All param met? Y	TCP/IP Uses DISN

Figure 7.3.6.8.6.2.F1. Information Needs for Plan Mission Process

Table 2-1A in Figure 7.3.6.8.6.2.F1 is an example of the Information Needs table for a defined Process or Activity, or in the example, the Plan Mission process. The column called "Info Need #" follows a number scheme for the Plan Mission process, where "O" represents *Operational Information Need* and "S" represents *System Information Method*. The numbering scheme will repeat for each separate process or activity. For example, in Table 2-1A, O1 and S1.1 will relate to that specific Process combination.

The following are the column headers and their descriptions in the Information Needs table for *Operational Information Needs*:

- *Info Need #*: Lists Operational Information Needs, following the number scheme described above.
- *Need Name*: Operational Information Need Name.
- *I/O*: Input or Output to the Process (I or O).
- *Producer*: Producing operational node name of this information need.
- *Consumer*: Receiving operational nodes name of this information need.
- *Minimum Parameters Ql | Qn | T | O*: The "X" signifies whether there are minimum parameters associated with quality (Ql), quantity (Qn), timeliness (T), or other (O) with this information need. No minimum parameters are designated by a dash (-).
- *Transport Methodology*: A dash (-) signifies that the transport methodology is only identified at the system level.

The following are column headers and their descriptions in the Information Needs table for *System Implementation Methods*:

- *Info Need #*: Lists System Information Methods, following the number scheme described above.
- *Need Name*: References the Supportability Assessment table for more information.
- *I/O*: A dash (-) signifies that Input or Output is only determined at the Operational Information Need level.
- *Producer*: Producing system node name of this information need.
- *Consumer*: Receiving system nodes name of this information need.
- *Minimum Parameters Ql | Qn | T | O*: The question "All param met?" will be followed by Y, No or Unk—yes, no, or unknown respectively—to indicate if all minimum parameters identified in the operational information level above are satisfactorily met using these particular system nodes and transport methodologies. Information will be expanded upon in the Supportability Assessment table.
- *Transport Methodology*: The transport methodology (i.e., Datalink, Transmission Control Protocol/Internet Protocol (TCP/IP), Voice or Other) used by these system nodes to pass information.

Supportability Assessment

Table 2-1B Supportability Assessment for Plan Mission Process

Info Need #	Parameter	Minimum Parameter	Need Met
S1.1		Operational area restriction Interface Implementation for Plan Mission Process	
S1.1	Quality	Accuracy 99%	N
S1.1	Size	Files cannot be larger than 10 MB	U
S1.1	Source PPT	< 1 Hr timelate	Y
S1.1	Operational Issue 1	Capability Not Within Parameter	
S1.1	Operational Risk 1	Briefings and Mission Plans File Size	
S3.1		Mine Warfare Plan Interface Implementation for Plan Mission Process	
S3.1		No Minimum Parameters ID'ed for this Operational Information Need	

Figure 7.3.6.8.6.2.F2. Supportability Assessment for Plan Mission Process

The Supportability Assessment table, Table 2-1B in Figure 7.3.6.8.6.2.F2, is an expansion of Minimum Parameters column from the Information Needs table, providing more detail on each of the system implementation methods, using the Info Need # as a reference. In Table 2-1B, the first row references System Implementation Method 1 (S1.1) from Table 2-1A. For each system implementation method identified in the Information Needs table, there is a corresponding section in the Supportability Assessment table.

The following are column headers and their descriptions in the Supportability Assessment table for system implementation methods:

- *Info Need #*: System Information Methods number from the Information Needs table.
- *Parameter*: The parameter being analyzed.
- *Minimum Parameter*: The metric that is required in order for this information need to be useful to the process.
- *Need Met*: Answers the question if the systems described in Table 2-1A (source/consumer system node or transport methodology) adequately support this information need in regards to the minimum parameter metric. Corresponding answers displayed will be Y, N, or Unk (yes, no, or unknown respectively).

If the Need Met column contains No and/or Unknown answers and if the ISP developer has provided details on the corresponding issue or risk, additional rows will appear identifying the operational issue/risk number and title. This is hyperlinked to Chapter 3.4 where further explanation is provided on the issue/risk.

Data Strategy Assessment

Table ***2-1C*** (8320.2) Data Strategy Assessment (TCP/IP Transport Methodology Implementations Only) for ***Plan Mission*** Process

Info Need #	Tagged	DDMS Registered	Web Service	Discoverable	IPV6	Other
S3.1	X			X		

Figure 7.3.6.8.6.2.F3. Data Strategy Assessment

The Data Strategy Assessment table in Figure 7.3.6.8.6.2.F3 is an expansion of the Transport Methodology column from the Information Needs table. If a system implementation method uses TCP/IP to pass information, then the Info Need # will appear in the Data Strategy Assessment table. If the system implementation method does not use TCP/IP to pass information, the table will display the message "No TCP/IP transport methodology was identified for this process/activity."

In the example Table 2-1C, System Implementation Method 1 from Table 2-1A and Table 2-1B displays which Data Strategy tenants are supported for all TCP/IP Transport.

7.3.6.8.6.3. Enhanced Information Support Plan (EISP) Feedback

EISP suggestions and recommendations are welcomed and should be submitted by email, using the Enhanced ISP Feedback form. Submit to eisp_help@bah.com.

7.3.6.9. Tailored Information Support Plan (TISP) Instructions

7.3.6.9. Tailored Information Support Plan (TISP) Instructions

TISP instructions are available from the Joint Staff (CJCS Instruction 6212.01).

7.3.6.9.1. Applicability

The Tailored Information Support Plan (TISP) is designed to improve the Information Support Plan (ISP) process by reducing the number of OSD-level reviews, streamlining the ISP waiver process, and providing a tailored ISP option for ACAT II, III and non-ACAT programs only.

7.3.6.9.2. Introduction

The Enhanced Information Support Plan (EISP) is designed to accommodate the Tailored Information Support Plan (TISP) and is encouraged as the tool for TISP development. Acquisition Category (ACAT) II and below, as well as Non-ACAT programs, may tailor the content of their Information Support Plan (ISP) upon Joint Staff J-6 approval. At a minimum, the tailored plan will provide explanation of the programs' Concept of Operations (CONOPS) and will provide IT supportability analysis of the CONOPS. Additionally, the following set of integrated architecture products is required: AV-1, OV-1 (optional), OV-5, OV-6C (optional), SV-1 (optional), SV-5, SV-6, and TV-1. The Program Manager will ask the Joint Staff J-6 what optional architecture products will be required via email. The Joint Staff J-6 will determine if optional views are required.

7.3.6.9.3. Tailored Information Support Plan (TISP) Pilot Program Process

TISP requests shall be requested via email to Joint Staff J-6 through the applicable Service/Agency/Joint Forces Command Interoperability Test Panel (ITP) representative. The

request will include: the program's name, description of the capability(ies) it provides, funding allocated to the program, and identification of key connectivity requirements (see Section 7.3.6.9.6, below, for submission format). Joint Staff J-6I will respond to the TISP request with a "Concur" or "Non-concur" via e-mail.

7.3.6.9.4. Approval of a Tailored Information Support Plan (TISP)

Approval of a TISP will be contingent on the following processes:

- If the mandatory sections of the form are not completed, the request will be returned to the submitter for completion.
- Joint Staff J-6I Net Readiness Assessment, Joint Capabilities Integration and Development System, and Enforcement/Testing branches shall review submitted TISP applications and make recommendation for approval or denial of TISP participation. The Joint Staff J-6I Division Chief retains final approval authority for entry into the TISP process.
- Applicants, and respective ISP representatives, will be notified via Joint C4I Program Assessment Tool - Enhanced that a program can precede with development of a TISP.

7.3.6.9.5. Tailored Information Support Plan (TISP) Preparation

- In accordance with DoD Instruction 4630.8, DoD Components/Agencies responsible for Information Support Plan (ISP) development shall comply with applicable portions of the instruction and the procedures outlined in the TISP Program. All TISP requests will be submitted to the appropriate DoD Combatant Command/Service/Agency (CC/S/A) Military Communications-Electronics Board Interoperability Test Panel (ITP) Representative using the format identified in Section 7.3.6.9.6, below (also available on the ITP web page for either on-line submission or downloading). The appropriate CC/S/A ITP Representative shall validate the TISP request.
- Upon DoD Component/Agency approval of using the TISP approach, the TISP will be submitted to Joint Staff J-6I via Joint C4I Program Assessment Tool - Enhanced by submitting their TISP to the appropriate DoD Component/Agency Interoperability Test Panel (ITP) representative point-of-contact for review, approval, and submittal.
- Joint Staff J-6I will coordinate with the Office of Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer on all submissions.
- As required, Joint Staff J-6I will invite the requesting system's Program Management Office or designated representative to the next scheduled ITP meeting to brief the members concerning the system and their justification for requesting a TISP instead of following DoD Instruction 4630.8 ISP procedures. The ITP will serve as an advisory panel to facilitate Joint Staff J-6I determination of system merits and means to mitigate interoperability certification issues.
- The TISP pilot program is intended to accelerate the Joint Interoperability Certification process, programs should make early contact with the Joint Interoperability Test

Command to create a testing strategy and gain technical points-of-contact for questions dealing with interoperability and supportability issues.

7.3.6.9.6. Tailored Information Support Plan (TISP) Request Form

Note: Send the completed form and required attachments to the appropriate DoD Combatant Command/Service/Agency (CC/S/A) Military Communications-Electronics Board Interoperability Test Panel (ITP) Representative. The CC/S/A Representative will validate the request and forward it through their Component Information Support Plan (ISP) representative who will post it on Joint C4I Program Assessment Tool - Enhanced for consideration.

A. PROGRAM INFORMATION

SYSTEM NAME: (Including system version number.)

Is this system to be employed within DSN or a PSTN? YES or NO

REQUESTING AGENT:

- COMMERCIAL PHONE NUMBER:
- DSN:

REQUESTING ORGANIZATION:

INTERNET EMAIL ADDRESS:

MAILING ADDRESS:

CITY/STATE/ZIP:

ALTERNATE POINT OF CONTACT (POC):

ALTERNATE POC COMMERCIAL TELEPHONE NUMBER:

Please insert pertinent information ONLY if different from above:

PM POC/NAME/RANK:

- Commercial phone number:
- DSN:
- Requesting Organization:
- Email Address:
- Address:

(DSN - Defense Telephone System Network; PTSN – Public Telephone System Network)

B. SYSTEM DESCRIPTION

Provide a written description of the system and a diagram identifying key operational nodes/system components.

Note: Use of additional information documents is encouraged (e.g., Concept of Operation; Mission Need Statement; Initial Capabilities Documents; Operational Requirements Documents; Test and Evaluation Master Plans; Capability Development Documents; Command, Control, Communication, Computers, and Intelligence Support Plans).

Note: You may include Web Pages and addresses where additional information can be found. Electronic versions are encouraged.

C. TISP QUESTIONS

1. What is the acquisition category (ACAT) of the program (ACAT I, II, III, non-ACAT)?
2. Is the program a rapid acquisition or legacy program?
3. What year was the program initiated?
4. What milestone is the program at (MS A, B, C, post-C)?
5. Has the program been tested by either the Service or Joint Interoperability Test Command? If so, provide a short summary of past testing efforts and copies of test reports.
6. What type of funding does this program have (provide details on future Operations and Maintenance, Procurement, and Research and Development funding)?
7. Does the program have any requirements documentation? If so what type?

D. JITC TESTING INFORMATION

1. Describe how many systems will be fielded.
2. Identify any joint connectivity requirements. Indicate other Service/Agency interfaces.
3. Provide a road map with a specific date of when you will be able to certify the system and whether it is currently scheduled for joint interoperability testing.
4. Identify the JITC POC who has been contacted for interoperability test coordination.
5. Provide any available test data to include Service/Agency test efforts.
6. Present any known problems or issues that could delay or prevent JITC certification.

7.3.6.10. Information Support Plan (ISP) Waiver Process

The requirement for an ISP may be waived when the requirement for Joint Capabilities Integration and Development System documentation has been waived, Joint Staff (J-6) has determined that the Net-Ready Key Performance Parameter or Interoperability Key Performance Parameter are not needed, or the program does not meet any of the criteria identified in

paragraphs 2.2.2, 2.2.3, and 2.2.4 of DoD Instruction 4630.8. Additionally, programs accepted under the Legacy System Interoperability Validation and Certificate Request Process are waived from producing an ISP.

Waiver requirements apply to all Acquisition Category (ACAT) and non-ACAT ISPs. Each DoD Component has an ISP waiver review process. Waiver requests shall be sent via email to Office of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) Computing and NetOps Directorate by the appropriate DoD Component action officer for coordination prior to approval. The waiver information will include: the program's name, the next milestone, the capability(ies) the program provides, list any external information and related connectivity, and the rationale for the waiver. ASD(NII)/DoD CIO will respond to the waiver request via memo indicating approval or disapproval. Waiver authority for non-ACAT ISPs resides with the cognizant fielding authority. Upon final approval by ASD(NII)/DoD CIO, the DoD Component will be provided a copy of the approved waiver. A test process is now in effect (currently the Navy only) to allow the component some waiver authority. This may be expanded. Legacy Waivers are defined in a ASD(NII)/DoD CIO memorandum and is being changed as reflected in the text below. As of this guidebook the following will apply for and be changed in future policy for legacy systems.

Fielded Legacy systems, ACAT II and below and non-ACAT programs, that meet all of the conditions outlined below may request a waiver from the Department of Defense (DoD) Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," dated May 5, 2004, requirement to produce an ISP. In addition to the standard ISP waiver, there are now two categories of legacy waivers with the qualifying conditions shown below by category:

- *Option A*: Permanent Legacy ISP Waiver.
    - Have no current validated Joint Staff requirements documentation;
    - Have no current interoperability test certification;
    - Have no pre-existing interoperability deficiencies identified by the Joint Interoperability Test Command (JITC);
    - Have no plan for funding beyond the Future Years Defense Program (FYDP); and
    - Will be out of the DoD inventory within 5 years.
- *Option B*: Four-year ISP Waiver. (This waiver provides a four-year, ISP waiver for fielded, non-ACAT I programs. At the end of the waiver period, the program may apply for an additional waiver, provided the program continues to meet the three-year waiver requirements.)
    - Have no current validated Joint Staff J-6 requirements documentation,
    - Lack a current interoperability test certification,
    - Have no major planned updates, incremental changes, spiral development changes planned.
    - Have no pre-existing interoperability deficiencies identified by the JITC.
    - Be funded beyond FYDP, with no established retirement date, and
    - Is currently connected to the Global Information Grid.

Waiver requests will follow the email-based waiver process described in CJCS Instruction 6212.01. When the ASD(NII)/DoD CIO has electronically approved the request, the fielded legacy system will follow the procedures established by the Joint Staff J-6, for interoperability certification and certificates to operate. Upon granting the waiver, the Joint Staff J-6 will inform ASD(NII)/DoD CIO of the approval.

7.4. Net-Centric Information Sharing Data Strategy

7.4. Net-Centric Information Sharing Data Strategy

The DoD Data Strategy is defined in DoD Directive 8320.02, "Data Sharing in a Net-Centric Department of Defense," December 2, 2004.

7.4.1. Implementing the DoD Net-Centric Data Strategy

The DoD Net-Centric Data Strategy (May 2003) outlines the vision for managing data in a net-centric information sharing environment. The strategy compels a shift to a "many-to-many" exchange of data, enabling many users and applications to leverage the same data—extending beyond the previous focus on standardized, predefined, point-to-point interfaces. Hence, the objectives are to ensure that all data are visible, available, and usable—when needed and where needed—to accelerate decision cycles. Specifically, the data strategy describes 7 major net-centric data goals as presented in Table 7.4.1.T1, below.

Goal	Description
Goals to increase Enterprise and community data over private user and system data	
Visible	Users and applications can discover the existence of data assets through catalogs, registries, and other search services. All data assets (intelligence, no intelligence, raw, and processed) are advertised or "made visible" by providing metadata, which describes the asset.
Accessible	Users and applications post data to a "shared space." Posting data implies that (1) descriptive information about the asset (metadata) has been provided to a catalog that is visible to the Enterprise and (2) the data is stored such that users and applications in the

	Enterprise can access it. Data assets are made available to any user or application except when limited by policy, regulation, or security.
Institutionalize	Data approaches are incorporated into Department processes and practices. The benefits of Enterprise and community data are recognized throughout the Department.
Goals to increase use of Enterprise and community data	
Understandable	Users and applications can comprehend the data, both structurally and semantically, and readily determine how the data may be used for their specific needs.
Trusted	Users and applications can determine and assess the authority of the source because the pedigree, security level, and access control level of each data asset is known and available.
Interoperable	Many-to-many exchanges of data occur between systems, through interfaces that are sometimes predefined or sometimes unanticipated. Metadata is available to allow mediation or translation of data between interfaces, as needed.
Responsive to User Needs	Perspectives of users, whether data consumers or data producers, are incorporated into data approaches via continual feedback to ensure satisfaction.

Table 7.4.1.T1. Net-Centric Data Strategy Goals

7.4.2. Implementing Net-Centric Data Sharing

7.4.2.1. The Roles, Responsibilities, and Relationships of the Community of Interest (COI) in Information Sharing

7.4.2.2. Community of Interest (COI) Formation and Execution

7.4.2.3. Data Sharing Implementation

7.4.2. Implementing Net-Centric Data Sharing

A DoD Guide, DoD 8320.2-G, "Guidance for Implementing Net-Centric Data Sharing," April 12, 2006, issued under the authority of DoD Directive 8320.02, "Data Sharing in a Net-Centric Department of Defense," December 2, 2004, provides implementation guidance for the community-based transformation of existing and planned information technology (IT) capabilities across the DoD. The goal of this Guide is to provide a set of activities that members of communities of interest (COIs) and associated leadership can use to implement the key policies of DoD Directive 8320.02 and ultimately increase mission effectiveness across the Department of Defense. The activities presented in this Guide may not apply to all COIs and should be tailored as necessary.

Implementation is largely achieved through activities conducted within Communities of Interests. This guidance covers some of the following key areas:

7.4.2.1. The Roles, Responsibilities, and Relationships of the Community of Interest (COI) in Information Sharing

See Chapter 2 in DoD 8320.02-G, "Guidance for Implementing Net-Centric Data Sharing," April 12, 2006.

Key COI Attributes

The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer "DoD Net-Centric Data Strategy," May 9, 2003, defines the COI as "a collaborative group of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange." COIs are organizing constructs created to assist in implementing net-centric information sharing. Their members are responsible for making information visible, accessible, understandable, and promoting trust – all of which contribute to the data interoperability necessary for effective information sharing. This chapter describes the roles, responsibilities, and relationships of COIs in information sharing.

The focus for COIs is to gain semantic and structural agreement on shared information. For COIs to be effective, their scope—that is, the sphere of their information sharing agreements—should be as narrow as reasonable given their mission. Although the Department of Defense or a Military Department might be considered a collaborative group of users who have a shared mission, and thus a COI, achieving a shared vocabulary across the entire Department of Defense or even across a Military Department has proved to be very difficult to achieve due to the scope and magnitude of the information sharing problem space. COIs represent a mechanism for decomposing the DoD's information sharing problem space into manageable parts that can be addressed by those closest to the individual parts.

COIs may be guided by the DoD's strategic goals, existing policy, and doctrine, or COIs may form on an ad hoc basis to address a data sharing problem among known stakeholders. While DoD Component-specific COIs may exist, COIs are most likely to be functional or joint entities that cross organizational boundaries. Examples of a COI might be a meteorology COI or a joint task force COI. COIs should include producers and consumers of data, as well as developers of systems and applications.

Although COIs may vary, the key attributes (below) should be applicable for the majority of COIs across the Department of Defense.

1. Formed to meet a specific data sharing mission or fulfill a task
2. Composed of stakeholders cooperating on behalf of various organizations, with emphasis on cross-Component activities

3. Members committed to actively sharing information in relation to their mission and/or task objectives
4. Recognize potential for authorized but unanticipated users and therefore, strive to make their data visible, accessible, and understandable to those inside and outside their community

7.4.2.2. Community of Interest (COI) Formation and Execution

7.4.2.2. Community of Interest (COI) Formation and Execution

See Chapter 3 in DoD 8320.02-G, "Guidance for Implementing Net-Centric Data Sharing," April 12, 2006.

This section provides a set of activities to help guide the establishment, evolution, and operations of a COI, as well as the fielding of real information sharing capabilities. Readers new to COIs, in the process of organizing a COI, or belonging to a newly-formed COI should consult this chapter. Members of short-term COIs or participants who are already familiar with the activities involved in organizing a community may wish to move on to section 7.4.2.3, which describes implementation of DoD Directive 8320.02, "Data Sharing in a Net-Centric Department of Defense," December 2, 2004.

COIs may take various forms and are not intended to be "one size fits all." These groups can differ in how they operate, the timelines for their actions, the duration of their existence, how they are governed, and whether or not they demonstrate information sharing capabilities through pilot activities before operational use. As such, COIs should determine what activities, and associated levels of effort, are necessary to ensure sufficient governance and management of the COI.

7.4.2.2.1. Establish and Evolve a Community of Interest (COI)

7.4.2.2.1.1. Activity Area Overview

The COI "Establish and Evolve" activity area focuses on identifying the purpose for a community, identifying the community's needs, and establishing a COI to work toward meeting those needs. The initial step in forming a COI is to identify a potential need for such a group, the mission, and potential membership. In addition, before establishing a new COI, potential members should identify other organizations and/or COIs that may be addressing the same or similar problem area.

If a similar COI exists and there is considerable semantic overlap in the identified problem area, potential members should reach out to the existing COI to leverage its work and investigate opportunities for collaboration. Assuming that a new COI is required, the process of establishing a new COI will involve the activities below. This section describes activities that aid implementation of the COIs referenced in paragraph 4.7 of DoD Directive 8320.02, "Data Sharing in a Net-Centric Department of Defense," December 2, 2004.

7.4.2.2.1.2. Implementation Activities

Identify mission, members, and desired information sharing capabilities. The initial membership of a Community of Interest (COI) will come together around a common information sharing mission that can be addressed as a community. The COI's mission can be formally articulated through a mission statement or charter if the members consider this appropriate. COIs can refer to guidance provided in Chapter 2 of DoD 8320.02-G to identify additional members. The COI should outline the purpose of the community and the scope of its activities, identifying key capabilities that enable the COI to accomplish its mission. Executing these steps ensures that COI agreements reflect end-user needs, that those agreements are technically viable to implement, and that they have the ownership and buy-in necessary to promote changes in operational programs and systems.

Identify related COIs. Communities should use the COI Directory, NII will fix or delete to identify related efforts for coordination of governance forums and sharing experiences. This directory maintains a listing of all DoD COIs that register, and provides visibility into their activities. Identification of other COIs can both inform the decision to establish a new COI and identify information sharing possibilities once a new COI has been established.

Prioritize information sharing capabilities. COIs should prioritize key capabilities to focus their efforts based on the potential mission value and feasibility of implementation. In identifying such information sharing capabilities, COIs should consider use of both new and legacy systems. Prioritization should help keep the scope of any COI-identified information sharing capabilities focused and facilitate the implementation of pilots, or initial operational capabilities, as quickly as possible. This enables the COI to contribute to the delivery of real value quickly while providing lessons learned before additional capabilities are developed.

Advertise the COI. To ensure that DoD users can discover the existence and mission of a COI and have the opportunity to participate, a member of the COI should register the COI in the COI Directory. To register, COIs should provide their name, point of contact, mission, status, COI lead, and proposed governing authority.

7.4.2.2.1.3. Forward Planning

Identify measures of success. Communities of interest (COIs) should define COI-specific success measures and measure progress against those criteria. Some measures will be mission specific. For example, success might be defined as reducing the time required to plan strikes as a result of having information available. Other measures of success might be non-mission specific. Non-mission specific measures can provide valuable insight enabling others in the Enterprise to assess data sharing approaches. For example, a COI could measure time saved in fielding new information sharing capabilities as a result of reusing existing data assets rather than re-creating data. Instituting measures of success helps ensure that the Enterprise continues to invest in those opportunities that provide value to the Enterprise.

Continually gather user feedback. COI members should strive to meet user needs, measure the value achieved through information sharing, and work with stakeholders to identify near-term information sharing capabilities. As the COI evolves, so will stakeholder priorities and needs. Periodically, members should reassess activities to ensure that the COI is continuing to provide value and that it continues to address the COI's mission with needed capabilities. This reassessment would include its support for net-centric information sharing across the Department of Defense. COI members should assess metric results to determine when the COI has achieved its mission and should disband or turn over operations to continuing organizations.

7.4.2.2.2. Community of Interest (COI) Management and Governance

7.4.2.2.2.1. Activity Area Overview

The COI "Management and Governance" activity area focuses on identifying a governing body, communicating with stakeholders, and providing leadership and direction to the COI. COI management and governance activities are integral to ensuring that COIs achieve their mission. Although these activities will be tailored to the individual COI's mission and the membership, there are basic issues that a COI should address. These issues include, but are not limited to,

information flow, issue adjudication, prioritization of COI activities, quality assurance, recommendations to portfolio managers, and configuration management of COI products. COI management is responsible for establishing governance processes and structures appropriate to the COI. This effort includes leveraging existing processes and structures where possible and appropriate.

A COI's ability to facilitate cross-Component portfolio management for Information Technology (IT) investments is essential for effective COI management. In IT portfolio management, designated Mission Area and sub-portfolio leads conduct reviews of DoD Component plans and budgets and ensure alignment and efficient use of resources that may advance COI-defined capabilities. As an example, the Intelligence Surveillance Reconnaissance (ISR) COI establishes the expectation that the DoD Components will support inter-Domain/inter-Component information sharing among the Distributed Common Ground System (DCGS) Family of Systems (FoS) program services. The ISR COI provides this direction through the prescribed use of common, shared, or federated information sharing services; specific data implementation strategies and tools, and COI specific agreement on access controls and security mechanisms. For subsequent portfolio reviews, the portfolio manager or identified COI governing authority bases the review on the ISR COI's guidance and works with the DoD Components to validate that each of the DCGS FoS programs are aligned and each has sufficient funding to effectively implement the COI-defined information sharing services and capabilities.

7.4.2.2.2.2. Implementation Activities

Identify governing authority. Communities of interest (COIs) should align themselves with an existing governing authority, such as a Mission Area lead, to enable the COI to impact the necessary related systems, programs, and data holdings. Mission Area leads may direct COIs to align themselves with a particular governing authority. Ideally, this governing authority should have flag or general officer level authority, without which the COI might lack the decision-making and resource authority to realize its information sharing goals. The governing authority should be in a position to influence agreements and to help address issues that affect multiple DoD Components.

Select a COI lead. The COI lead is the point of contact and action officer for COI activities. This role differs from that of the governing authority in that the COI lead is responsible for the day-to-day functioning of the COI but should be in a position to influence agreements and to help address issues that affect multiple DoD Components. The COI lead interfaces with the COI governing authority to report status, resolve issues, promote COI agreements, and to make recommendations on DoD Component's plans and schedules. Other responsibilities include leading regular meetings; establishing working groups, as needed; identifying other potential members; acting as a liaison to the portfolio manager or other governing authority; coordinating with the relevant program or system managers; collaborating with other COIs to reuse metadata artifacts; and helping to mitigate any conflict within the COI.

Establish COI-specific governance processes. COIs should develop internal governance processes or leverage existing processes appropriate to the scope and mission of the COI. These activities include appropriate review and adjudication of issues and establishment of Memorandums of Agreement or Memorandums of Understanding as a set of working agreements among participants and their respective organizations. In addition, COI governance processes should enable the establishment of working groups, as needed, to address COI focus areas. For example, the COI might task a data working group with developing COI categorization schemes, thesauri, vocabularies, and taxonomies. COIs should ensure that their working groups operate with defined timelines, focus area(s), and deliverables.

Clarify relationships between groups involved in the COI. Although COI members share a mission, establishing a clear understanding of information sharing relationships among members rather than assuming that such an understanding already exists will help shape COI responsibilities and direction.

Share COI information with all stakeholders. An important aspect of management and governance is transparency of information. COI members should communicate with one another and the governing authority, as well as with their respective organizations. To this end, COIs should track and publicize their activities, schedules, actions, and progress. In addition, COIs should provide stakeholders with the results of specific metrics and measurements (i.e., assessment of performance against metrics) including progress in implementing new information sharing capabilities and progress towards implementing policy according to DoD Directive 8320.02, "Data Sharing in a Net-Centric Department of Defense," December 2, 2004.

This process includes involving stakeholders in the review of documents and specifications developed by the COI and providing the community with mechanisms for user feedback.

Assess reusability of other resources. Using the DoD Metadata Registry, communities should identify opportunities for semantic and structural metadata reuse. COIs should also consult other COIs for opportunities to capitalize on operational data access services that can enrich their data sets and, potentially, be integrated into their data sharing capabilities (e.g., a COI can build a new capability using another COI service that is already in place).

Forward Planning. COIs should plan for the long-term maintenance of COI metadata artifacts, including taxonomies and schemas, in consideration of other organizations that have built services that depend on these artifacts. For COIs that are not planned for long-term continuation, the COI should consult with the lead DoD Component organization or governing authority to develop a plan for long-term maintenance, to include configuration management.

7.4.2.2.3. Community of Interest (COI) Capability Planning and User Evaluation

7.4.2.2.3.1. Activity Area Overview

COIs play a key role in implementing net-centric data sharing across the DoD. The mission-focused and typically joint nature of COIs enable the identification and development of net-centric information sharing capabilities that are of greatest value to DoD users. Through pilots and operational information sharing capabilities, members of COIs can demonstrate the mission value of using cross-Component data sources.

The "Capability Planning and User Evaluation" activity area focuses on defining an information sharing capability that the COI needs, working with DoD Components to implement the capability, and integrating it into ongoing operations. In some cases, COIs, through their members and associated programs, systems, and data sources, may develop pilot capabilities before engaging in full deployment of a capability. When planning for information sharing capabilities, COI members should define a set of requirements for the capability developers (associated with a program of record or organization with data assets and budget). Associated programs of record inform DoD processes as appropriate when planning for information sharing capabilities. Capability developers are responsible for turning the requirements into a physical implementation of data assets and services in accordance with COI agreements.

The overall goal of these activities is to assist a COI to evolve net-centric information sharing capabilities. Through these activities, COIs should actively identify information sharing needs and work to integrate new capabilities supporting known needs of the COI, as well as providing readily discoverable and understandable information to authorized but unanticipated users.

7.4.2.2.3.2. Implementation Activities

Identify the approach for delivering the capabilities. Community of Interest (COI) members must consider the normal certification and test processes when determining whether information sharing capabilities will be piloted or offered for operational use. The COI should base its approach on many factors, including technical and operational risk and the life-cycle stage of the data assets involved. For example, a COI may decide to develop a pilot capability that exposes data from existing systems in order to create a new asset before pursuing operational fielding of the capability. Leveraging exposed data from existing systems (instead of targeting programs in the new cycle), may enable the COI to field a capability faster and provide more immediate benefits to users.

Define measures of success. The COI's members should identify measures of success, including performance and resource-usage improvements. These measures should include metrics that can be used to assess the operational performance as well as provide insight into possible improvements in capability delivery (e.g., time to field, impacts on existing assets). When choosing to implement a pilot capability, it is important to assess whether the pilot effort will generate the intended capability to support the COI's mission, and whether the pilot capability technical solution can be integrated into the operational capability with a minimum of integration difficulty.

Create a capability plan. COIs, in collaboration with the appropriate stakeholders, should develop a capability plan, including a schedule and identification of the data assets of programs, systems, and organizations to be tagged and exposed. Additionally, the plan should include resource requirements; any intermediate demonstrations, pilot efforts, and tests that must be performed; and operational integration tasks. The capability plan should be communicated with the governing authority, system and data asset owners, and other COI stakeholders. Implementation of the plan can then be carried out by participating programs and their respective capability developers. Communications should include measures of success to evaluate capability implementation and user satisfaction.

7.4.2.2.3.3. Forward Planning

Evaluate the capability. During capability execution, Communities of interest (COIs) should extend success criteria to evaluate the overall impact of the information sharing capability on the mission objectives and the overall value of the effort to the Department of Defense. The COI should evaluate capability planning and execution in two ways, which are described above, and then capture lessons learned, also as described above.

Develop measures and metrics. In addition to metrics developed through the capability planning effort, COIs should develop metrics to assess the COI's progress relative to the DoD goals of net-centric information sharing and whether implementation resulted in a meaningful return on investment (ROI). In this instance, ROI indicates that the benefiting DoD Component or program of record has saved money by not having to build a new system to handle and re-create newly shared data. Other measures of ROI could include reduced cycle time and improved legal compliance. The COI should document the costs of implementation to provide a measure of the investment and should include a baseline assessment of relevant data assets to determine future capabilities.

Check user satisfaction. As part of the ongoing feedback loop, COIs should make data regarding the information sharing capability implementation available and accessible to consumers of the community's data, and gather input from these users. Gathering consumer, or user, input will enable the COI to gauge user satisfaction and determine whether the capability meets user needs and expectations.

Capture lessons learned by the COI. Capturing and communicating lessons learned is a key part of the COI's governance responsibilities. Lessons learned provide current and future best practices, baseline financial data, and provide other valuable insight into the fielding of new information sharing capabilities. Although there is no one-size-fits-all approach, COIs should leverage all available resources to avoid repeating past mistakes and duplicating current efforts. COIs should also plan to meet regularly with the appropriate portfolio manager and other stakeholders to review implementation results.

7.4.2.3. Data Sharing Implementation

7.4.2.3. Data Sharing Implementation

See Chapter 4 in DoD 8320.02-G, "Guidance for Implementing Net-Centric Data Sharing," April 12, 2006.

Making data visible, accessible, and understandable, and promoting trust in the data are the cornerstones of net-centric information sharing. The creation of duplicative data and redundant capabilities often results from consumers' inability to locate, access, understand, or trust that existing data assets meet their needs. This chapter describes activities to guide Communities of interest (COIs) in implementing information sharing.

The activities described in this chapter should not be interpreted as a rigid sequence. Some tailoring of the associated activities by individual COIs is expected and encouraged. Regardless of the steps taken, COIs should strive to fulfill their primary responsibilities.

7.4.2.3.1. Making Data Visible

Making data visible focuses on creating discovery metadata and deploying discovery capabilities that catalog data assets for users to find. The overall goal of data visibility is to enable DoD users to sift through the enormous volume and variety of DoD information holdings and quickly discover data assets that pertain to specific subjects of immediate interest. Discovery capabilities providing discovery metadata enable consumers to find out who is responsible for specific assets, where the assets are located, what kind of data is available, and how to go about accessing them.

The discovery metadata may also include elements defined as COI extensions described in the in the DoD Discovery Metadata Specification (DDMS).These elements are related to the subject matter of the data asset, and are necessary for specialist consumers in a particular subject matter to locate relevant data assets. The activities presented in the following paragraphs help implement policy goals of paragraph 4.2 of DoD Directive 8320.02, "Data Sharing in a Net-Centric Department of Defense," December 2, 2004.

7.4.2.3.1.1. Implementation Activities

Identify data assets to share. Members of the community of interest (COI) should build a prioritized list of the data assets it will initially make visible to the Department of Defense. The list should include descriptive information on each of the identified data assets such as POC information, including email addresses and telephone numbers; name of proposed or existing data access service and any related information resources; and a high-level narrative description. The primary candidates for the initial visibility effort should be the COI's current operational data assets, followed by mature developmental capabilities that are on a rapid deployment track to fill known mission data gaps and information needs. Prioritization occurs at the COI's discretion, taking into consideration organizational preparedness, technical ease of service implementation, law, policy and security classification restrictions, impact of broader access on the COI's operations, and the quantitative and qualitative improvements that might result from making a particular data asset visible.

Define and register COI extensions for discovery metadata. One core purpose for COIs is to foster agreements on the meaning and physical representation of their data assets, as packaged and offered in deployed services. This includes the agreement on any metadata necessary to properly describe the community's data assets. The DoD Discovery Metadata Specification (DDMS) provides the minimum discovery metadata requirements to support enterprise discovery of data assets and can be extended by COIs to provide additional context that aids in the search for relevant data assets.

- *Enterprise Considerations.* The COI is in the position to anticipate how users might want to find data assets, in part based on the data assets' context or content. Supplementing the rudimentary discovery metadata elements, such as "Creator" or "Classification" found in the DDMS core, the COI extensions detail elements of discovery metadata that aid in enterprise-wide discovery of data assets related to that COI.
- *Technical Guidance.* COI extensions to the DDMS may take the form of a data schema, and as such should be registered in the DoD Metadata Registry, as part of the COI's set of

agreed upon metadata artifacts. Formatting and technical guidance for COI extensions can be found in the DDMS.

Leverage work from other COIs. COIs should leverage the DoD Metadata Registry to access guidance on technical, organizational, and procedural approaches to data asset publication. Other available information includes specific DDMS extensions registered by other COIs, data schemas for carrying product payload, taxonomies, and other data engineering artifacts. These models can provide a starting point for the COI efforts to reach agreement on common elements that will be important for users to discover COI data assets. Additional information regarding COIs that have registered metadata in the DoD Metadata Registry may be available in the COI Directory.

Associate discovery metadata with data assets. The association of discovery metadata with data assets is also referred to as "data tagging" within the context of data visibility. Data visibility is enhanced through the use and publication of discovery metadata that describe data assets. The implementation of "data tagging" mechanisms may vary by data asset and granularity of description. COI members should discuss possible methods of associating discovery metadata with capability developers or establish a COI working group to consider the issue and provide recommendations. In this way, the COI can determine the appropriate methods for the types of data assets the COI makes visible.

- *Enterprise Considerations.* Extensible Markup Language (XML)-based discovery metadata is the most flexible means of sharing discovery metadata throughout the Department of Defense.
- *Technical Guidance.* To illustrate the distinction between physical and logical tagging and association of metadata, consider the example of a data asset in the form of a single file, such as a DoD Directive. Physically tagging a file would mean placing discovery metadata elements directly into that file, alongside its content. In contrast, logically associating discovery metadata with the file would involve creating a separate file, possibly XML based, containing discovery metadata that describes the file. Software automation of this task is highly recommended; however, the precise mechanism will depend on the type of data asset and granularity of description. The DDMS provides the minimum required structure and content for discovery-related tags. By adhering to this specification for tagging, the minimum necessary discovery metadata to participate in federated searches will be available.

Create a discovery capability containing discovery metadata. Each COI should consult its governing authority to identify the information and resources associated with providing a discovery capability that the COI can use for its discovery metadata. The purpose of a discovery capability is to provide DDMS-formatted discovery metadata in response to federated searches. Capability developers will then leverage the COI's discovery metadata in the discovery capability, allowing authorized users to discover the COI's data assets.

- *Enterprise Considerations.* COIs should consult the enterprise specifications for data asset discovery. By complying with these enterprise discovery specifications, the COI helps ensure the interoperability of its discovery capability with the discovery capabilities of other groups and, ultimately, helps enable Enterprise-wide federation of discovery services. Federated discovery services give authorized DoD users the richest set of data assets from which to discover relevant data to meet their mission needs.
- *Technical Guidance.* COIs can access the Defense Information Systems Agency Net-Centric Enterprise Services visibility guidance, which provides more specific technical guidance for discovery capabilities. COIs should use available and mature federated search specifications to ensure that discovery capabilities interoperate with the Enterprise properly. Enterprise discovery specifications also include requirements for service discovery. Service discovery metadata typically takes the form of a Universal Description, Discovery, and Integration description of a web service. COIs can also consult with other COIs, or other existing resources, for implementations of discovery capabilities and gain insights into the use of similar technology across the Department of Defense.

7.4.2.3.1.2. Forward Planning

Communities of interest (COIs) should establish, as part of its plan for long-term maintenance of COI metadata artifacts, a plan for maintaining the discovery metadata, the COI extensions to the DoD Discovery Metadata Specification, and the service discovery metadata. The goal is to make data visible as soon as possible and to develop those resources over time. The COI should agree on a schedule and process for how it will maintain the discovery metadata, to ensure that the data is always the most current.

7.4.2.3.1.3. Making Data Accessible

Making data accessible focuses on offering data assets over the network through commonly supported access methods. This goal of Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))/DoD Chief Information Officer (CIO) Memorandum ""DoD Net-Centric Data Strategy," May 9, 2003, deals with providing methods for obtaining data that both humans and machines can use, except where limited by law, policy, or security classifications. While making data visible involves creation and use of discovery metadata, making data accessible refers to providing access to the underlying information provided by the data asset so that authorized DoD users can make use of it. Taking into account the "post before processing" paradigm, the COI should make data assets available as soon as possible and should not delay making the data accessible in order to complete processing of data prior to posting it.

This section describes activities that aid in implementing paragraph 4.3 of DoD Directive 8320.02, "Data Sharing in a Net-Centric Department of Defense," December 2, 2004.

Individually negotiated interfaces between systems are brittle and inflexible; they support only the information transfers anticipated during development, not the "pull-on-demand" transfers that are a key part of net-centric data sharing. While point-to-point interfaces will continue to exist, ASD(NII)/DoD CIO Memorandum "DoD Net-Centric Data Strategy," May 9, 2003, emphasizes the need to transition those interfaces and implement new interfaces to support many-to-many information exchanges and authorized but unanticipated users. Data producers should make data assets accessible using web-based approaches, minimizing the need for predefined, engineered point-to-point interfaces wherever operationally and technically possible.

7.4.2.3.1.3.1. Examples of Making Data Accessible

- Providing a website displaying imagery for an Area of Responsibility for humans to use. (This example describes a method through which humans can get information.)
- Providing a web service through which a computer application can obtain imagery data in support of situation awareness. (This example describes a method through which a computer can retrieve raw sensor image data.)
- Providing a web service that an application can use to determine the flight trajectory of a missile. (This example describes a method for computer access to a process or calculation.)

7.4.2.3.1.3.2. Implementation Activities

Understand data sharing constraints. The community of interest (COI) should identify any existing policies, laws, or data classifications that would restrict access to the data across the Enterprise. Traditional data access mechanisms will contain many implicit rules indicating how systems respond to requests, based on how the requests fall into a predefined process for handling the requests. Therefore, in addition to identifying explicit restrictions on data access, the COI should also consider the potential for (and attempt to discern) built-in role-based access control systems. COIs should maintain awareness of evolving DoD information assurance, information security, and information sharing policies, and incorporate them as appropriate into COI activities and implementations.

Discover enterprise resources. The COI should leverage work products of other COIs, operational data access mechanisms that are available, and available net-centric interface standards and specifications.

- *Enterprise Considerations.* The COI can promote access mechanism reuse, and minimize the work required to obtain desired capabilities by collaborating with other COIs. In addition, the COI can make its own data accessible on an enterprise scale by adhering to existing technical standards. Interfaces developed using standard interface specifications enable COI-developed access mechanisms to exchange information readily with enterprise services resulting in wider access to the community's data assets.

- *Technical Guidance.* The Key Interface Profiles are the set of documentation produced as a result of interface analysis that designates an interface as key; analyzes it to understand it's architectural, interoperability, test, and configuration management characteristics; and documents those characteristics in conjunction with solution sets for issues identified during analysis.

Identify data assets to make accessible. The COI should determine which assets within the associated organizations, programs of record, sub-portfolios, etc., are likely to be of most value to those inside and outside the COI taking into account the potential for authorized but unanticipated users. The data assets that the COI makes accessible will typically be a necessary component of the new information sharing capability identified by the COI.

- *Enterprise Considerations.* Part of the value of net-centric information sharing lies in its ability to afford authorized but unanticipated users with access to data, as needed. Taking this into account, COIs should assess information sharing options with the understanding that there might be other consumers in the DoD, external to the COI, who could make valuable use of the COI's data.

Define requirements for access mechanisms. The COI should define the priority of and functional requirements for data access mechanisms. Depending on the situation, the COI may base these requirements on an existing data access mechanism or establish them as part of an ongoing implementation plan. In setting requirements for data access mechanisms, the COI should take into account the type of assets; the security, license, and privacy considerations; and the static, dynamic, or streaming nature of data change. The data access mechanism specifications should conform to any agreements put forward by the stakeholders and the COI.

- *Technical Guidance.* The specific technology architecture of data access mechanisms will depend on a number of factors, including the nature of the underlying data asset, whether humans or machines will consume the asset, and the operational scenarios that surround the asset's use. Preferred architectures will use web-based technologies based on open standards, such as web services, portals, and web pages using Hypertext Markup Language and common web display standards. The DoD Information Technology (IT) Standards Registry (DISR), according to DoD Directive 4630.05, provides the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements whose purpose is to ensure that a conformant system satisfies a specified set of requirements. The standards and guidelines in the DISR are stable, technically mature, and available via DISRonline.

Post descriptions of access mechanisms. Capability developers in the COI should publish metadata for any data access mechanisms to available service registries, so that both known and authorized but unanticipated users may discover the service and understand how to interact with it.

- *Enterprise Considerations.* Publication of access mechanisms has two enterprise benefits: the first is enabling unanticipated users to find the service; the second is providing all background information necessary to reuse the service, deterring the development of redundant services.
- *Technical Guidance.* In the case of web services, enterprise specifications should be consulted for the minimum service discovery requirements to enable enterprise-wide discovery of COI data services. For instance, additional information in the form of a Universal Description, Discovery, and Integration description may be required to enable federated discovery and greater understanding of data services.

7.4.2.3.1.3.3. Forward Planning

Review systems for operational impact and scalability. Communities of interest should not degrade system performance for critical operational users to make data accessible. In addition, access mechanisms should be engineered for maximum scalability.

Develop expandable systems. Although such mechanisms need not immediately support the entire set of DoD users, they must be expandable to meet growth in demand.

7.4.2.3.1.4. Making Data Understandable

Making data understandable focuses on reaching agreement on the meaning of information provided by data asset,s and making that understanding available to consumers through the DoD Metadata Registry. Data that is visible and accessible is still not usable unless it is understandable. The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer Memorandum "DoD Net-Centric Data Strategy," May 9, 2003, provides for the existence of expedient communities of interest (COIs) that may have diverse data needs, based on operational requirements. It is therefore not always safe to assume that data consumers will be familiar with what a COI's data means, the way it is structured, or particularly how it fits into the COI's operational context. Most important, it is not necessarily the case that all consumers will be using data in the same way or for the same purpose. For example, "a tank" in the Army might refer to an armored vehicle, whereas "a tank" in the Navy might refer to a storage device for fluids. Although the data producer's perspective might be reasonable within the producer's context, the consumer might have a very different purpose in mind.

This section describes activities that aid in implementation of paragraphs 4.4, 4.6, and 4.7 of DoD Directive 8320.02, "Data Sharing in a Net-Centric Department of Defense," December 2, 2004.

7.4.2.3.1.4.1. Implementation Activities

Discover enterprise resources. As part of developing a shared understanding of the community of interest's (COI) data, the COI should discover existing enterprise resources in order to maximize reuse of existing metadata artifacts.

Gather existing semantic metadata. The DoD Metadata Registry will contain vocabularies, taxonomies, ontologies, conceptual data schemas, and other forms of semantic metadata from other COIs upon which the COI might base development of its own semantic metadata. In addition, the COI should discover existing semantic metadata among its members. In this way, the COI can start the process with a foundation in related semantics.

Gather existing structural metadata. The DoD Metadata Registry also contains logical and physical data schemas that could aid the COI in forming structural representations that would be understandable to end-users. Data asset structure (such as whether dates are represented as normal, or as Julian dates) is an important aspect of understanding. By using the DoD Metadata Registry and consulting COI members, the COI can start the process with a foundation in related structures.

Develop a shared understanding of COI data made visible. COI members, pooling subject matter expertise, should collaborate on several semantic metadata artifacts that are crucial for providing context and meaning to any COI data that is made visible and accessible.

Agree on a shared vocabulary. The COI should use its own extensions to the DoD Discovery Metadata Specification as a starting point for the shared vocabulary. As a set of terms and definitions, the shared vocabulary should include any term used in the COI extensions, along with definitions that put these and other terms into proper COI context.

Agree on a conceptual data schema. The conceptual data schema indicates high-level data entities. Its coverage includes any entities in visible COI data assets, as well as the relationships between those data entities. The conceptual schema's coverage area may include multiple data assets, requiring that the COI come to an agreement on how members will collaborate, possibly through a COI data working group, to develop the conceptual schema.

Agree on a COI taxonomy. A COI taxonomy is a categorization hierarchy indicating generalization and specialization relationships between terms; a submarine is a kind of sea-based asset, and an Abrams M1A1 is a kind of tank.

- *Enterprise Considerations.* Metadata artifacts such as the shared vocabulary, conceptual data schema, and taxonomy will be necessary for data consumers to understand a COI's data and to relate concepts within it. These artifacts will play a vital role in allowing mediation between COIs. The conceptual data schema indicates the general data subject area for consumers who are attempting to discover data assets relevant to their purpose.

Associate format- and content-related metadata. Content-related metadata is specifically aimed at providing content details, such as topics, keywords, context, and other information. Format-

related metadata refers to how the data asset is formatted or represented. It is important that data assets use formats that are understandable to data consumers. The COI should agree on how these metadata elements will be associated with data assets, using the DoD Discovery Metadata Specification as the specification for guidance on specific elements that will be associated with data assets.

- *Enterprise Considerations.* Content metadata provides a basis for search engines to locate data assets by keyword or topic, and improves the human understandability of the data. Format-related metadata enables consumers to determine whether or not they can consume a data asset. COIs should avoid the use of less well known publication formats that require special software. A good, understandable publication format will be one that is widely known and for which no additional software for conversion to a more widely known format is required.
- *Technical Guidance.* For content-related metadata, relevant DDMS elements are located in the Subject category. For format-related metadata, recommended formats are typically open and common throughout the enterprise, such as Joint Photographic Experts Group imagery, MP3 audio files, Apple Quick Time videos, and Microsoft Office document formats.

Register the Metadata Artifacts. Registration of semantic and structural metadata within the DoD Metadata Registry enables all users both anticipated and unanticipated to discover their existence, access them, and establish an understanding of the meaning and context of COI data.

- *Enterprise Considerations.* Registration of metadata artifacts enables unanticipated users and those outside the COI to discover the meaning and context of COI data and facilitates their reuse across the Department of Defense.
- *Technical Guidance.* Registering these artifacts means posting them to the DoD Metadata Registry. The COI can accomplish this by accessing the DoD Metadata Registry and following the instructions for submission.

7.4.2.3.1.4.2. Forward Planning

Determine how the community of interest (COI) will maintain metadata artifacts. As the COI develops over time, the shared vocabulary, COI taxonomy, and other metadata artifacts that enable understandability should remain synchronized with the subject area they represent. To help it attain this objective, a COI could institute rules relating to how shared vocabulary updates occur. In addition, COI governance should be consulted for configuration management standards and related maintenance schedules.

- *Enterprise Considerations.* Unanticipated users will require and rely on up-to-date metadata artifacts to help them understand the context of discovered data assets and properly assess their relevance to their current mission.

Improve the understandability of the data. The first iteration of metadata artifacts for understandability need not be ideal, since the goal is to make data assets available as soon as possible, rather than to have a perfect vocabulary on the first try. COIs should plan on improving their artifacts over time. Understandability is improved by providing more and better semantic metadata artifacts that capture and convey the knowledge consumers require to correctly use the data.

Anticipate future mediation needs. Mediation is the process of reconciling one vocabulary with, or translating one vocabulary to, another. The need for such mediation is inevitable in an environment with many different systems and representation languages. By tracking which types of mediation occur or will occur most frequently, the COI can aggregate best practices surrounding the mediation of its data with other sources, as well as gain an understanding of what format and structural issues may exist. The COI should register metadata artifacts necessary for mediation in the DoD Metadata Registry, which will facilitate their discovery and usage.

Ensure that data structure meets the consumers' needs, including those of unanticipated users. The physical structure of the data affects how the consumer will understand and utilize the data. Because it is not possible to know the unanticipated uses and needs of the data, COIs can engage in ongoing planning to change the structure of the data as it is exposed to the consumer via the access mechanism. Note that this sort of change represents a change to the access mechanism, not necessarily a change to the underlying data asset. Such changes can be meaningful only if they are made with consideration for user feedback.

7.4.2.3.1.5. Promoting Trust

A consumer that can locate, access, and understand a particular data asset, will want to assess the authority of the data asset to determine whether the contents can be trusted. Promoting trust focuses on identifying sources clearly and associating rich pedigree and security metadata with data assets to support the consumer's trust decision.

While COIs can promote trust through implementation of the activities described in this section, this Guidebook does not provide COIs the authority to share information in any way that is prohibited by law, policy, or security classification.

This section describes activities that aid in implementation of paragraph 4.5 of DoD Directive 8320.02, "Data Sharing in a Net-Centric Department of Defense," December 2, 2004.

7.4.2.3.1.5.1. Implementation Activities

Identify authoritative data sources. The community of interest (COI) should make every effort to identify data assets that are authoritative sources for data, as well as identifying in what contexts the data is authoritative. In situations where there is more than one authoritative source,

depending on how the data is used, the COI should indicate the business process for which the authority is valid.

- *Enterprise Considerations.* The COI should consider the ownership and stewardship of data sources when determining authoritativeness. Active stewardship will help maintain the quality and relevance of authoritative data sources for those internal and external to the COI.
- *Technical Guidance.* Authoritative sources may vary by COI (e.g., one community may define an authoritative source for location data to be the United States Postal Service, whereas another community might define an authoritative source for location data to be an intelligence database). In addition, a community might define more than one authoritative source for a particular type of data (e.g., a budget and planning community might have an authoritative source for budget data for each Military Department).

Associate trust discovery metadata with data assets. The COI should include trust discovery metadata to support data consumers' decisions on which community data assets are appropriate for their use. There are three categories of trust discovery metadata. These are discussed in the following subparagraphs.

- *Asset pedigree metadata.* The source and lineage of an asset are its pedigree. The purpose of the pedigree is to enable consumers to determine whether the asset is fit for their intended use and to enable them to track the flow of information, its transformations, and modifications, through assets. Notional metadata describing an asset's pedigree would include creation date, modification date, processing steps (including methods and tools), source and author (if known) status, and validation results against a published set of constraints.
- *Security labels.* Security labels provided in discovery metadata enable services to restrict access to data assets on the basis of a COI's identified parameters, including classification and dissemination controls. Preventing unauthorized access to data assets is important to promote trust in the data among authorized users.
- *Associate rights protection metadata.* Rights protection metadata refers to metadata that indicates any copyright, trademark, licensing, proprietary information, privacy act, or other usage restriction. As such, it may not be appropriate for all assets. Nevertheless, where this metadata does apply, it is important that it be provided. Consumers and data access services can only protect data against inappropriate use if they are informed of restrictions.
- *Technical Guidance.* The DoD Discovery Metadata Specification (DDMS) references the security elements found in the Intelligence Community Metadata Working Group document, specifying 18 attributes that can be used for information in classification and controls marking. The DDMS category named "Security" contains relevant elements addressing classification and dissemination. The "Source" category contains elements for asset pedigree metadata, and the "Rights" category contains applicable elements for rights protection metadata. The COI can obtain background on security tagging by checking the

Intelligence Community Metadata Standard for Information Security Markings and accessing the Data Element Dictionary.

7.4.2.3.1.5.2. Forward Planning

Because a data asset can be trusted only if its contents are sufficiently accurate and of sufficiently reliable quality, assessing and improving data asset quality is important. Quality assertions about data include information on its accuracy, completeness, or timeliness for a particular purpose. For example, consumers might need to know the age of the data to determine whether it is trustworthy, or they might need to know how accurate estimates and figures within the data asset are. Typically, such metadata results from a separate data quality analysis of an asset. The community of interest (COI) may develop an ongoing process for auditing the quality of data assets that are made visible and accessible. This process should be designed in concert with the COI leadership's ongoing quality assurance and configuration management efforts.

7.4.3. Integrating Net-Centric Information Sharing into the Acquisition Life Cycle

7.4.3. Integrating Net-Centric Information Sharing into the Acquisition Life Cycle

A description of the program's approach for ensuring that information assets will be made visible, accessible, and understandable to any potential user as early as possible (DoD Directive 8320.02, "Data Sharing in a Net-Centric Department of Defense," December 2, 2004"). This approach will be updated at subsequent milestones, will be summarized in the acquisition strategy, and will be described in more detail in the Information Support Plan. Recommended scope of activities follow:

7.4.3.1. Data Planning Activities

Define Net-Centric Data Sharing Plan

This activity relates to the development of a comprehensive net-centric plan to share data assets within your program/organization and to the Enterprise. This includes metadata catalog plans, registry plans, interoperability plans, etc. In essence, this Net-Centric Data Sharing Plan should be the program's/organization's plan to accomplish the goals of the DoD Net-Centric Data Strategy. This is a key product and will drive most data activities and architectures.

Responsibilities: Sponsor/Domain Owners should develop these plans at a broad, strategic level to ensure that architectures for programs and sub-organizations associated with the Domain include net-centric data components. Depending on the scale of the program or system, Program Managers (PMs) should develop a more detailed data sharing plan that outlines how their information architecture(s) make their data and processes discoverable, accessible, and understandable to both known and unanticipated users. These program data sharing plans should ensure that they align with and make use of enterprise net-centric data sharing capabilities such as those envisioned/planned under core enterprise services.

Define Data Guidance

Evaluate information from sources such as compliance reports, incentive plan reports, policy, and user needs to create net-centric data guidance documents. Data guidance is the policy, specifications, standards, etc, used to drive data activities within the program/organization. It differs from a net-centric data plan in that the plan is more strategic in nature. Data guidance may be a subset of an overall net-centric data sharing plan.

Responsibilities: Sponsor/Domain Owners should develop appropriate issuance and standards to ensure that incentives, metrics, and direction are in place to drive the transition to net-centricity. Sponsor/Domain Owners should establish policy and governance to ensure that the Domain's Programs and sub-organizations have a voice in the development of standards, specifications, and processes (e.g., empowering a Program to insert its metadata requirements into an overall Domain metadata model).

Define Net-Centric Information Sharing Data Architectures

Build upon existing and revised architectures and plans to describe the architecture to support data sharing objectives. The architecture should depict components that emphasize the use of discovery, services-based approach to systems engineering, use of metadata to support mediated information exchange, web-based access to data assets, etc.

Responsibilities: Both Sponsor/Domain Owners and PMs should include net-centric concepts, activities, and processes into their architectures. Sponsor/Domain Owners should ensure that their Domain-level architectures are developed in a manner that is appropriate for governing under a capabilities-based portfolio management process. PMs should ensure that net-centric components are integrated into their program architecture products.

7.4.3.2. Data Planning

Identify Data Assets

Determine what data assets (documents, images, metadata, services, etc) are produced or controlled within a program or organization. This is primarily an inventory of data assets, which should include both structured and unstructured data sources.

Responsibilities: Sponsor/Domain Owners should identify major data assets created or managed within their Domain. This asset listing will assist in the development of visibility, accessibility, and understandability strategic plans (i.e., based on the composition of the major data assets within the Domain, the planning products can reflect the most appropriate approach in supporting net-centric information sharing data strategy goals). Likewise, Program Managers (PMs) should inventory the data assets created or managed by the program and use this asset listing to plan their strategy and implementation approach for making these assets net-centric.

Prioritize Data Assets

Assess the data asset inventory to identify key data products that are of greatest value to known users and are likely to be of value to unanticipated users. This list should be used to determine data assets a program/organization should make initial efforts at exposing as enterprise data assets.

Responsibilities: Both Sponsor/Domain Owners and PMs should analyze and prioritize which data assets are most valuable, initially, to be exposed as enterprise data assets.

Define Communities of Interest (COIs)

Identify appropriate groups of people who should come together to support common mission objectives. COIs are an appropriate construct for defining information exchange formats and metadata definitions as well as vocabularies used to communicate within the COI. This activity does not include the 'establishment' of actual COIs. This is simply the process of identifying COIs that exist or should exist.

Responsibilities: Sponsors/Domain Owners should define major COIs that could benefit missions within the Domain (and across Domains). PMs should identify other COIs that serve the goals of the program and its associated functional areas.

7.4.3.3. Manage Data Infrastructure [Determine Infrastructure Requirements]

Manage Discovery Metadata Catalog(s)

Identifying/establishing and maintaining searchable catalogs used to locate data assets within the program, organization, or enterprise. Metadata stored within these catalogs facilitates discovery and includes descriptive information about each shared data asset.

Responsibilities: Sponsor/Domain Owners should establish Domain-level metadata catalogs that allow for the search of data assets across the Domain. Distributed, federated approaches should be used in developing this capability. Program Managers (PMs) should ensure that their data is tagged and posted to metadata catalogs that are tied into the Domain metadata catalog.

Manage Metadata Registry(s)

Identifying and/or establishing metadata registries that can be used to maintain, manage, and/or search for metadata artifacts such as schema and data definitions. Metadata stored in metadata registries are typically for developers, business analysts, and architects. Metadata registries are a type of metadata catalog specifically designed to support developers/business analysts.

Responsibilities: Sponsor/Domain Owners should ensure that metadata products within their Domain (including associated programs and sub-organizations) are registered into the DoD Metadata Registry. Domain Communities of Interest (COIs) are likely to be structured around the functional areas for which metadata is registered. PMs should ensure that program metadata is registered in the DoD Metadata Registry and is maintained.

Manage Service Directory(s)

Identifying and/or establishing service directory(s) that can be used to maintain, manage, and/or search for callable, reusable services from which net-centric capabilities are built. Metadata stored in service directories gives information as to the services available, how to call them, and possibly, expected service levels. Service directories include Universal Description, Discovery, and Integration Directories used to maintain Web Services information. This is a key component of establishing a services-based architecture that supports net-centric data tenets.

Responsibilities: Sponsor/Domain Owners should ensure that services created or managed within their Domain (including associated programs and sub-organizations) are registered into the DoD NCES Service Registry maintained by the Defense Information Systems Agency. PMs should ensure that program services are registered in the DoD NCES Service Registry.

Manage Interoperability Components

Development of metadata artifacts used to enable the interchange of data and information including document vocabularies, taxonomies, common data models, schema, formats, mediation components, and interface specifications.

Responsibilities: Sponsor/Domain Owners should establish Domain-level metadata models to facilitate the loosely-coupled exchange of information between systems. PMs should develop metadata models (e.g., data structures, schema, etc) pertinent to their program. This includes tagging models, service schema, and mapping models to the Domain metadata model.

Develop/Acquire Data Access Mechanism(s)

Post data assets to an information sharing application (e.g., end-user web site, a file system, a document repository) or through the use of web services to provide system-to-system access, etc.

Responsibilities: Sponsor/Domain Owners should establish shared space, as necessary, to support Program's within its scope. PMs should ensure that web-enabled services provide access to valuable systems data and processes.

Manage COIs

This activity encompasses establishing COI(s), registering COI(s) in the Enterprise COI Directory, and COI participation. The outcomes of this activity will ensure that COI(s) can be located and managed throughout the enterprise.

Responsibilities: Both Sponsor/Domain Owners and PMs should establish, register, and maintain identified COIs.

7.4.3.4. Provide Enterprise Data Assets

Provide Discovery Metadata

Associate or generate discovery metadata for data assets. This activity is the 'tagging' of data assets to provide value-added information about data assets that can be used to support discovery, accessibility, information assurance, and understandability.

Responsibilities: Program Managers (PMs) should ensure that discovery metadata is provided for all data assets created/managed by the Program.

Post Discovery Metadata

Providing, or posting, discovery metadata to catalogs, registries, etc, that can be searched. It is through 'posting metadata' that metadata catalogs are populated. This activity allows data assets to be discovered (but does not guarantee access to the data asset).

Responsibilities: PMs should ensure that discovery metadata associated with each data asset is posted to searchable metadata catalogs (established by the Domain and by Programs).

7.4.3.5. Govern Data Activities

Participate in DoD Information Enterprise (DoD IE) Governance

Participate in governance activities that enable net-centric data asset sharing. This includes participation in DoD IE Enterprise Service efforts, net-centric architectural compliance, Capabilities Portfolio Management for net-centric information sharing, etc.

Responsibilities: Sponsor/Domain Owners should participate in DIE governance activities to ensure the proper processes are followed and executed within their Domain to enable the net-centric Domain environment.

Enforce Data Guidance

Participate in enforcement/compliance activities that assess net-centric architectures against Net-Centric Data Guidance that was developed in the Data Planning process.

Responsibilities: Both Sponsor/Domain Owners and PMs should enforce established data guidance (including conformance to standards and adherence to DoD/Domain issuances).

Advocate Data Strategy(s)

This activity involves vetting, publicizing, and institutionalizing the Net-Centric Data Sharing plans and guidance developed in the Data Planning process.

Responsibilities: Both Sponsor/Domain Owners and PMs should advocate the DoD Net-Centric Data Strategy and Domain-established data guidance.

7.4.4. Supporting Language for Information Technology (IT) System Procurements

To ensure support of the goals of DoD Net-Centric Data Strategy, the Program Manager (PM), through his or her contracting specialists, should include the following sections, as appropriate, in Request for Proposal (RFP)/Request for Quotation (RFQ) language for the procurement of IT systems.

The contractor shall ensure that any IT systems covered in this procurement or identified in this RFP/RFQ support the goals of the Defense Information Enterprise Architecture 1.1 dated May 27, 2009 and its subsequent official updates and revisions. The contractor shall ensure that any IT systems covered in this procurement or identified in this RFP/RFQ support the goals of the DoD Net-Centric Data Strategy dated May 9, 2003, and comply with the Department's data strategy as defined in DoD Directive 8320.02, "Data Sharing in a Net-Centric Department of Defense", December 2, 2004. The contractor shall ensure that any IT systems covered in this procurement or identified in this RFP/RFQ support the goals of DoD Net-Centric Services Strategy, Strategy for a Net-Centric, Service Oriented DoD Enterprise, March, 2007.

Also, the contractor must ensure that any IT systems covered in this procurement or identified in this RFP/RFQ meet the requirements detailed below. Additionally, it is acceptable for vendors and/or integrators to provide functionality (via wrappers, interfaces, extensions) that tailor the COTS system to enable these requirements below (i.e., the COTS system need not be modified internally if the vendor/integrator enables the requirements through external or additional

mechanisms. In this case, these mechanisms must be acquired along with the COTS system procurement).

- Access to Data: *The contractor shall ensure that all data managed by the IT system can be made accessible to the widest possible audience of DIE users via open, web-based standards. Additionally, the system's data should be accessible to DIE users without 1) the need for proprietary client-side software/hardware, or 2) the need for licensed user-access (e.g. non-licensed users should be able to access the system's data independent to the licensing model of the COTS system). This includes all data that is used to perform mission-related analysis and processing including structured and unstructured sources of data such as databases, reports, and documents. It is not required that internal, maintenance data structures be accessible.*
- Metadata: *The contractor shall ensure that all significant business data made accessible by the IT system is tagged with descriptive metadata to support the net-centric goal of data visibility. Accordingly, the system data shall be tagged to comply, at a minimum, with the DoD Discovery Metadata Specification (DDMS). This specification is available at: https://metadata.dod.mil/mdr/homepage.htm. The system should provide DDMS-compliant metadata at an appropriate level based on the type of data being tagged. It is not required that individual records within databases be tagged; rather it is expected that the database itself or some segment of it is tagged appropriately. Additionally, the contractor shall ensure that all structural and vocabulary metadata (metamodels, data dictionaries) associated with the exposed system data be made available in order to enable understanding of data formats and definitions. This includes proprietary metadata if it is required to effectively use the system data.*
- Enterprise Services/Capabilities: *The contractor shall ensure that key business logic processing and other functional capabilities contained within the IT system are exposed using web-based open standards (e.g., application programming interfaces provide for Web Services-based access to system processes and data). The level of business logic exposure shall be sufficient to enable reuse/extension within other applications and/or to build new capabilities. The contractor shall provide an assessment of how any licensing restrictions affect or do not affect meeting the goals of re-use and exposure as DoD Information Enterprise-wide enterprise services.*
- Optional Components/Modules: *The contractor shall ensure that all standard and/or optional components of the IT system are identified and procured in a manner that ensures the requirements outlined in this document are met.*

7.5. Information Assurance (IA)

7.5.1. Information Assurance (IA) Overview

Most programs delivering capability to the warfighter or business domains will use information technology to enable or deliver that capability. For those programs, developing a comprehensive and effective approach to IA is a fundamental requirement and will be key in successfully achieving program objectives. The Department of Defense defines IA as "measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities." DoD policy and implementing instructions on information assurance are in the 8500 series of DoD publications. Program Managers and functional proponents for programs should be familiar with statutory and regulatory requirements governing information assurance, and understand the major tasks involved in developing an IA organization, defining IA requirements, incorporating IA in the program's architecture, developing an acquisition IA strategy (when required), conducting appropriate IA testing, and achieving IA certification and accreditation for the program. The information in the following sections will explain these tasks, the policy from which they are derived, their relationship to the acquisition framework, and the details one should consider in working towards effective IA defenses-in-depth in a net-centric environment.

7.5.2. Mandatory Policies

7.5.2.1. DoD Directive 5000.01, "The Defense Acquisition System"

Paragraph E1.9, "Information Assurance," states:

Acquisition managers shall address information assurance requirements for all weapon systems; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems; and information technology programs that depend on external information sources or provide information to other DoD systems. DoD policy for information assurance of information technology, including NSS, appears in DoD Directive 8500.1….

7.5.2.2. DoD Instruction 5000.02, "Operation of the Defense Acquisition System"

Table 8, "Title 40/CCA Compliance," in enclosure 5 requires the following of acquisition program managers:

Ensure that the program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards.

7.5.2.3. DoD Directive 8500.01E, "Information Assurance (IA)"

This directive establishes policy and assigns responsibilities under 10 U.S.C. 2224 to achieve DoD information assurance through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare. According to DoD Directive 8500.01E, all acquisitions of DoD Information Systems (to include Automated Information System applications, Outsourced Information Technology-based Processes, and platforms or weapon systems) with connections to the Global Information Grid must be certified and accredited.

7.5.2.4. DoD Instruction 8500.2, "Information Assurance (IA) Implementation"

This instruction implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks under DoD Directive 8500.01.

7.5.2.5. DoD Instruction 8580.1, "Information Assurance (IA) in the Defense Acquisition System"

This instruction implements policy, assigns responsibilities, and prescribes procedures necessary to integrate information assurance (IA) into the Defense Acquisition System; describes required and recommended levels of IA activities relative to the acquisition of systems and services; describes the essential elements of an Acquisition IA Strategy, its applicability, and prescribes an Acquisition IA Strategy submission and review process.

7.5.2.6. DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)"

This instruction establishes the DoD information assurance (IA) certification and accreditation (C&A) process for authorizing the operation of DoD information systems consistent with the Federal Information Security Management Act and DoD Directive 8500.01E. The instruction supersedes DoD Instruction 5200.40 (DITSCAP) and DoD 8510.1-M (DITSCAP Manual). The new DIACAP process supports net-centricity through an effective and dynamic IA C&A process. It also provides visibility and control of the implementation of IA capabilities and services, the C&A process, and accreditation decisions authorizing the operation of DoD information systems, to include core enterprise services and web services-enabled software systems and applications.

7.5.2.7. DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)"

NOTE: DoD Instruction 5200.40 has been superseded by the issuance of DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)." The process described in DoD Instruction 5200.40, however, shall be followed for those systems permitted to gradually transition to the DIACAP.

DoD Instruction 5200.40 implements policy, assigns responsibilities and prescribes procedures under DoD Directive 8500.01E for Certification and Accreditation of information technology, including automated information systems, networks, and sites in the Department of Defense.

7.5.2.8. Other Processes

Other Certification and Accreditation processes (such as Director of Central Intelligence Directive (DCID) 6/3 "Protecting Sensitive Compartmented Information within Information Systems") are applicable for systems processing Sensitive Compartmented Information.

7.5.3. Information Assurance (IA) Integration into the Acquisition Life Cycle

7.5.3.1. Before Milestone A

Examine program and system characteristics to determine whether compliance with DoD Directive 8500.01E is recommended or required, and whether an acquisition Information Assurance (IA) strategy is required. (Click here for guidelines on making this determination.)

Establish an IA organization. Appoint a trained IA professional in writing as the IA Manager. This and other IA support may be organic to the program office, matrixed from other supporting organizations (e.g., Program Executive Office), or acquired through a support contractor.

Begin to identify system IA requirements. Click here for Baseline IA Controls or IA Requirements Beyond Baseline Controls.

Develop an acquisition IA strategy, if required. Click here for IA Compliance Decision Tree or click here for an Acquisition IA Strategy Template. Acquisition IA strategies developed in preparation for Milestone A will be more general, and contain a lesser level of detail than acquisition IA strategies submitted to support subsequent Milestone decisions. Click here to see the detailed Acquisition IA Strategy guidelines.

7.5.3.2. Before Milestone B

If program is initiated post-Milestone A, complete all actions for Milestone A.

Ensure Information Assurance (IA) considerations are incorporated in the program's Acquisition Strategy. Click here for example language for Acquisition Strategy IA Considerations.

Update and submit the acquisition IA strategy. Click here for an Acquisition IA Strategy Template.

Secure resources for IA. Include IA in program budget to cover the cost of developing, procuring, testing, certifying and accrediting, and maintaining the posture of system IA solutions. Ensure appropriate types of funds are allocated (e.g., Operations & Maintenance for maintaining IA posture in out years).

Initiate the DoD Information Assurance Certification and Accreditation Process (DIACAP), or other applicable Certification & Accreditation process (such as Director of Central Intelligence Directive (DCID) 6/3 "Protecting Sensitive Compartmented Information within Information Systems" for systems processing Sensitive Compartmented Information).

7.5.3.3. Before Milestone C

Incorporate Information Assurance (IA) solutions through:

- Employment of Information Systems Security Engineering (ISSE) efforts to develop or modify the IA component of the system architecture to ensure it is in compliance with the IA component of the Global Information Grid architecture, and makes maximum use of enterprise IA capabilities and services.
- Procurement of IA/IA enabled products. DoD Instruction 5000.02, paragraph 6 of Enclosure 5, states that: "When the use of commercial IT is considered viable, maximum leverage of and coordination with the DoD Enterprise Software Initiative shall be made." The Enterprise Software Initiative (ESI) includes commercial IA tools and should be utilized as the preferred source for the procurement of IA tools. The ESI Home Page lists covered products and procedures. DFARS (SUBPART 208.74) lists additional requirements for compliance with the DoD ESI.
- Implementation of security policies, plans, and procedures.
- Conducting IA Training.

Test and evaluate IA solutions. Click here for IA Testing details.

- Developmental Test.
- Security Test & Evaluation, Certification and Accreditation activities.
- Operational Test.

Accredit the system under the DIACAP or other applicable Certification and Accreditation process. For systems using the DIACAP, an Authorization to Operate should be issued by the Designated Accrediting Authority.

7.5.3.4. After Milestone C or before the Full Rate Production Decision Review (or equivalent for MAIS Programs)

Maintain the system's security posture throughout its life cycle. This includes periodic re-accreditation.

Assess IA during IOT&E on the mature system.

7.5.4. Estimated Information Assurance (IA) Activity Durations and Preparation Lead Times

Figure 7.5.4.F1 shows the relationship between the acquisition framework and typical timeframes for accomplishing key IA activities.

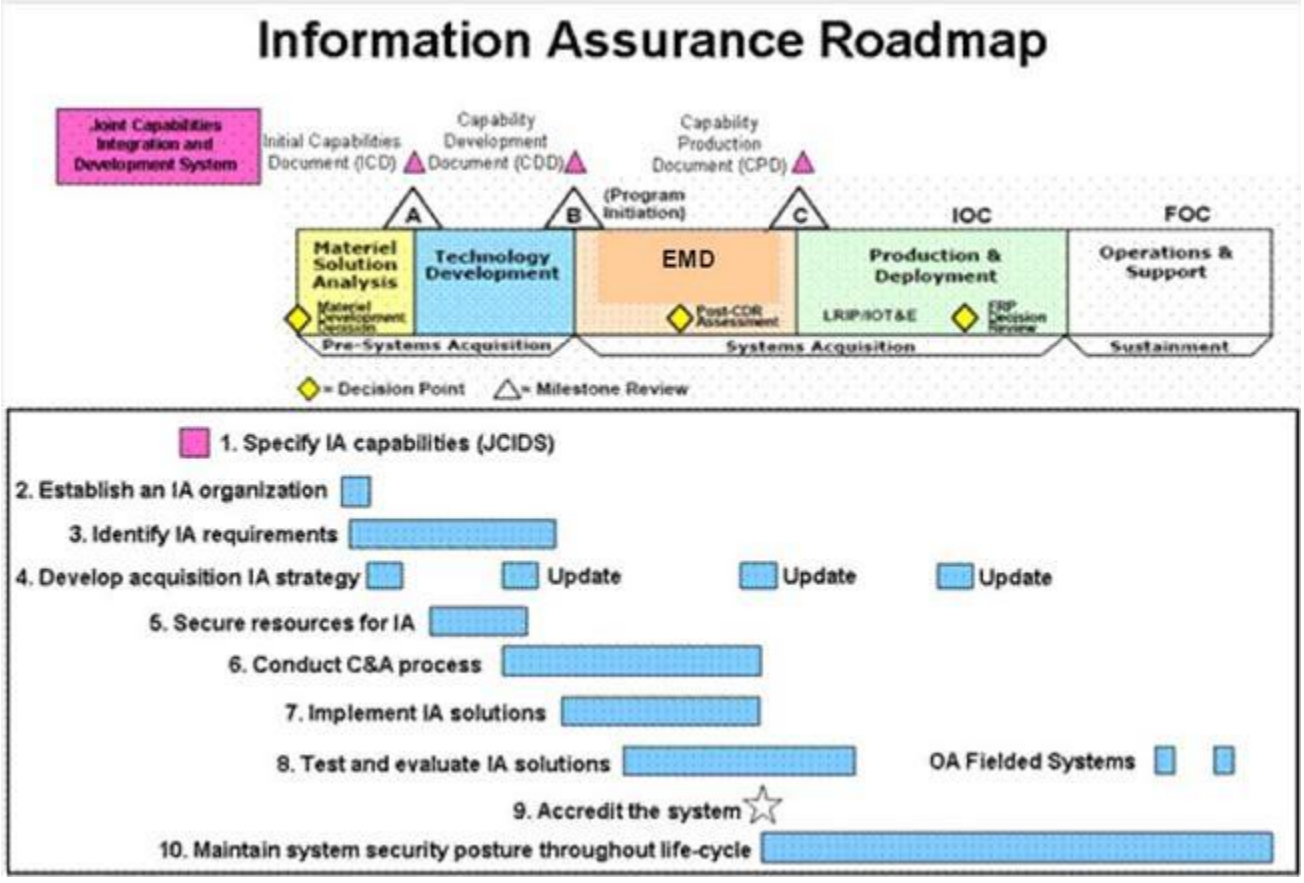


Figure 7.5.4.F1. Typical Timeframes for Accomplishing Key IA Activities

7.5.5. Integrating Information Assurance (IA) into the Acquisition Process

Table 7.5.5.T1, IA Compliance by Acquisition Program Type, is designed to help program managers determine the degree to which the 8500 series applies to a system acquisition and whether an Acquisition IA Strategy is required.

Acquisition Programs for:		Acquisition IA Strategy	Compliance with Table 7.5.5.1. IA Compliance by
No IT		Not Required	Not Required
Non-MC/ME AIS		Not Required*	Required
Non-MC/ME MAIS		Not Required*	Required
MC/ME AIS		Required	Required
MC/ME MAIS		Required	Required
Outsourced IT-based Processes		Not Required*	Required
Outsourced IT-based Processes that are MC/ME		Required	Required
Platform IT products/weapons systems that are, or have:			
MC/ME	Network Interconnections to the GIG		
No	No	Not Required*	*Recommended***
No	Yes	Not Required*	Required
Yes	No	Required	*Recommended***
Yes	Yes	Required	Required

Legend:
AIS = Automated Information System
GIG = Global Information Grid
IT = Information Technology
MAIS = Major Automated Information System
MC/ME = Mission Critical/Mission Essential
PM = Program/Project Manager

* Although not required by DoD, the Component may require an Acquisition IA Strategy.
** PMs would be prudent to comply with all DoDI 8500.2 IA controls appropriate to the system

Table 7.5.5.T1. IA Compliance by Acquisition Program Type

Because requirements for IA vary greatly across acquisition programs, program managers should examine acquisition programs carefully to identify applicable IA requirements. The following guidelines derived from DoD Directive 8500.01E apply:

1. Programs that do not involve the use of Information Technology (IT) in any form have no IA requirements. Program managers should carefully examine programs, however, since many programs have IT (such as automatic test equipment) embedded in the product or its supporting equipment.
2. Programs that include IT always have IA requirements, but these IA requirements may be satisfied through the normal system design and test regimen, and may not be required to comply with DoD Directive 8500.01E. Acquisitions that include Platform IT with no network interconnection to the Global Information Grid fit into this category. However,

such programs require an IA Strategy if they are designated Mission Critical or Mission Essential.

3. Acquisitions of Platforms with network interconnections to the Global Information Grid must comply with the IA requirements of DoD Directive 8500.01E and DoD Instruction 8500.2.
4. Acquisitions of Automated Information System applications or outsourced IT processes also must comply with DoD Directive 8500.1 and DoDI 8500.2.
5. Programs that include IT, and that are designated Mission Critical or Mission Essential, require an IA Strategy without regard to the applicability of DoD Directive 8500.01E. The DoD Component Chief Information Officer is responsible for approving the IA Strategy. Subsequent to the DoD Component Chief Information Officer approval, in accordance with DoD Instruction 8580.1, the DoD Chief Information Officer must review the IA Strategy.

7.5.6. Program Manager (PM) Responsibilities

7.5.6.1. Platform Information Technology (IT) Systems

Program Managers (PMs) for acquisitions of platforms with internal IT (including platforms such as weapons systems, sensors, medical technologies, or utility distribution systems) remain ultimately responsible for the platform's overall Information Assurance (IA) protection. If the Platform IT has an interconnection to the Global Information Grid (GIG), in accordance with DoD Instruction 8500.2, the PM must identify all assurance measures needed to ensure both the protection of the interconnecting GIG enclave, and the protection of the platform from connection risks (such as unauthorized access), that may be introduced from the enclave. However, connecting enclaves have the primary responsibility for extending needed IA services (such as Identification and Authentication) to ensure an assured interconnection for both the enclave and the interconnecting platform. These IA requirements should be addressed as early in the acquisition process as possible.

PMs for acquisitions of Platforms with IT that does not interconnect with the GIG retain the responsibility to incorporate all IA protective measures necessary to support the platform's combat or support mission functions. The definition of the GIG recognizes "non-GIG IT that is stand-alone, self-contained or embedded IT that is not or will not be connected to the enterprise network." Non-GIG IT may include "closed loop" networks that are dedicated to activities like

weapons guidance and control, exercise, configuration control or remote administration of a specific platform or collection of platforms. The primary test between whether a network is part of the GIG or is non-GIG IT is whether it provides enterprise or common network services to any legitimate GIG entity. In any case, program managers for systems that are not connected to GIG networks would demonstrate prudent judgment by considering the IA program provisions in DoD Directive 8500.01E and DoD Instruction 8500.2, and employing those IA controls appropriate to their system.

7.5.6.2. Automated Information Systems (AIS)

Program Managers (PMs) for acquisitions of AIS applications are responsible for coordinating with enclaves that will host (run) the applications early in the acquisition process to address operational security risks which the system may impose upon the enclave, as well as identifying all system security needs that may be more easily addressed by enclave services than by system enhancement. The baseline Information Assurance (IA) Controls serve as a common framework to facilitate this process. The Designated Approving Authority for the enclave receiving an AIS application is responsible for incorporating the IA considerations for the AIS application into the enclave's IA plan. The burden for ensuring that an AIS application has adequate assurance is a shared responsibility of both the AIS application PMand the Designated Approving Authority for the hosting enclave; however, the responsibility for initiation of this negotiation process lies clearly with the PM. PMs should, to the extent possible, draw upon the common IA capabilities that can be provided by the hosting enclave.

7.5.6.3. Outsourced Information Technology (IT)-based Processes

Program Managers (PMs) for acquisitions of Outsourced IT-based Processes must comply with the Information Assurance (IA) requirements in the 8500 policy series. They are responsible for delivering outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services that present specific and unique challenges for the protection of the Global Information Grid. The PM for an Outsourced IT-based process should carefully define and assess the functions to be performed and identify the technical and procedural security requirements that must be satisfied to protect DoD information in the service provider's operating environment and interconnected DoD information systems.

A unique type of Outsourced IT-based Process is "Managed Enterprise Services." These are defined as "Private sector information systems, outsourced information technologies, or outsourced information services managed, maintained and administered as a performance-based service (whether delivered from vendor facilities or within DoD facilities) that delivers a DoD-wide service included within the Enterprise Information Environment Mission Area (EIEMA), as an outsourced IT-based process." Managed Enterprise Services envision two broad categories of implementation scenarios:

- In one scenario, the service is hosted at vendor facilities, and accordingly, DoD does not have significant control of the operations of the Managed Enterprise Service.
- In the second scenario, the Managed Enterprise Service is hosted in a DoD facility, but operations are provided by one or more vendors. Managed services that are DoD Component-wide or that belong to the warfighter or business mission areas are outside the scope of Managed Enterprise Services. If your acquisition includes Managed Enterprise Services, see DoD CIO Memorandum "Certification and Accreditation Requirements for DoD-wide Managed Enterprise Services Procurements," dated June 22, 2006.

7.5.6.4. Privacy Impact Assessment (PIA)

A PIA is an analysis of whether personally identifiable information (PII) when collected in electronic form is stored, shared, and managed in a manner that protects the privacy of individuals. Section 208 of Public Law 107-347 requires that a PIA be conducted prior to developing or purchasing any DoD information system that will collect, maintain, use, or disseminate PII about members of the public, federal personnel, DoD contractors and, in some cases, foreign nationals. A DoD CIO memo and PIA Template provide procedures for completing and approving PIAs in the Department of Defense.

7.5.7. Information Assurance (IA) Controls

7.5.7.1. Mission Assurance Category (MAC) and Confidentiality Level

DoD Instruction 8500.2, Enclosure 3, establishes fundamental IA requirements for DoD information systems in the form of two sets of graded baseline IA Controls. Program Managers are responsible for employing the sets of baseline controls appropriate to their programs. The baseline sets of IA controls are pre-defined based on the determination of the Mission Assurance Category (MAC) and Confidentiality Levels as specified in the formal requirements documentation or by the User Representative on behalf of the information owner. IA Controls addressing availability and integrity requirements are keyed to the system's MAC based on the importance of the information to the mission—particularly the warfighters' combat mission. IA Controls addressing confidentiality requirements are based on the sensitivity or classification of

the information. There are three MAC levels and three confidentiality levels with each level representing increasingly stringent information assurance requirements. The three MAC levels are identified in Table 7.5.7.1.T1.

MISSION ASSURANCE CATEGORY			
	DEFINITION	Integrity	Availability
1	These systems handle information that is determined to be **vital to the operational readiness or mission effectiveness of deployed and contingency forces** in terms of both content and timeliness.	HIGH	HIGH
2	These systems **handle information that is important to the support of deployed and contingency forces**.	HIGH	MEDIUM
3	These systems handle information that is necessary for the conduct of day-to-day business, but **does not materially affect support to deployed or contingency forces in the short-term**.	BASIC	BASIC

Table 7.5.7.1.T1. Mission Assurance Category (MAC) Levels for IA Controls

The other major component in forming the baseline set of IA controls for every information system is determined by selecting the appropriate confidentiality level based on the sensitivity of the information associated with the information system. DoD has defined three levels of confidentiality, identified in Table 7.5.7.1.T2.

Confidentiality Level	Definition
Classified	Systems processing classified information
Sensitive	Systems processing sensitive information as defined in DoD Directive 8500.01E, to include any unclassified information not cleared for public release
Public	Systems processing publicly releasable information as defined in DoD Directive 8500.01E (i.e., information that has undergone a security review and been cleared for public release)

Table 7.5.7.1.T2. Confidentiality Levels for IA Controls

7.5.7.2. Baseline Information Assurance (IA) Controls

The specific set of baseline IA controls that the program manager should address is formed by combining the appropriate lists of Mission Assurance Category (MAC) and Confidentiality Level controls specified in the DoD Instruction 8500.2. Table 7.5.7.2.T1 illustrates the possible combinations.

Combination	Mission Assurance Category	Confidentiality Level	DoDI 8500.2 Enclosure 4 Attachments
1	MAC 1	Classified	1 and 4
2	MAC 1	Sensitive	1 and 5
3	MAC 1	Public	1 and 6
4	MAC 2	Classified	2 and 4
5	MAC 2	Sensitive	2 and 5
6	MAC 2	Public	2 and 6
7	MAC 3	Classified	3 and 4
8	MAC 3	Sensitive	3 and 5
9	MAC 3	Public	3 and 6

Table 7.5.7.2.T1. Possible Combinations of Mission Assurance Category and Confidentiality Level

There are a total of 157 individual IA Controls from which the baseline sets are formed. Each IA Control describes an objective IA condition achieved through the application of specific safeguards, or through the regulation of specific activities. The objective condition is testable, compliance is measurable, and the activities required to achieve the objective condition for every IA Control are assignable, and thus accountable. The IA Controls specifically address availability, integrity, and confidentiality requirements, but also take into consideration the requirements for non-repudiation and authentication.

It is important to exercise due diligence in establishing the MAC level of an information system. The baseline set of IA controls for availability and integrity are purposefully graded to become increasingly stringent for the higher MAC levels. The required resource costs to achieve compliance with the baseline IA controls at the higher MAC levels can be very significant as befits information and information systems on which a warfighter's mission readiness or operational success depends. The IA controls also become increasingly stringent or robust at the higher Confidentiality levels.

7.5.7.3. Information Assurance (IA) Requirements Beyond Baseline IA Controls

There are several additional sources of IA requirements beyond the Baseline IA Controls.

A system being acquired may have specific IA requirements levied upon it through its controlling capabilities document (i.e., Capstone Requirements Document, Initial Capabilities Document, Capability Development Document, or Capability Production Document). These IA requirements may be specified as performance parameters with both objective and threshold values.

All IA requirements, regardless of source, are compiled in the system's DoD Information Assurance Certification and Accreditation Process (DIACAP) Implementation Plan (similar to the system Requirements Traceability Matrix used in the DoD Information Technology Security Certification and Accreditation Process, superseded by the DIACAP). The DIACAP Implementation Plan documents all IA controls and requirements assigned, whether implemented or "inherited," and for each displays the implementation status, resources required, and the estimated completion date.

7.5.7.4. Security Pre-Configuration of Global Information Grid (GIG) Information Technology (IT) Components

To prevent exposing the GIG to avoidable vulnerabilities, all IT components (both hardware and software), for which security guidelines and enhanced configuration management processes have been developed, should be pre-configured before their connection to the GIG (i.e. integrated/connected to a DoD Automated Information System, enclave/network, or platform IT).

The Department regularly publishes security configuration guidelines enabling IT components to deliver the highest level of inherent security. These guidelines can be obtained from the following sites: Security Technical Implementation Guides from the Defense Information Systems Agency, and Security Configuration Guides from the National Security Agency.

The pre-configuration of GIG IT components to the appropriate security configuration guideline by the vendor should be made a preference in selecting components for procurement. To implement this, solicitations should specify the relevant guideline, and evaluation factors for award should include pre-configuration as a factor. Requiring activities should coordinate with their supporting contracting office to determine the appropriate weight for this factor. Note that this is preference, not a mandatory requirement.

Regardless of whether GIG IT components are procured and delivered in a pre-configured state, system managers and IA managers are responsible for ensuring that IT components (both

hardware and software), for which security guidelines have been developed, are appropriately configured prior to their installation/connection to the GIG.

7.5.8. Information Assurance (IA) Testing

See section 9.9.2.

7.5.9. Acquisition Information Assurance (IA) Strategy

7.5.9. Acquisition Information Assurance (IA) Strategy

The primary purpose of the Acquisition IA Strategy is to ensure compliance with the statutory requirements of Title 40/Clinger-Cohen Act and related legislation, as implemented by DoD Instruction 5000.02. As stated in Table 8 , Enclosure 5, of that instruction, the Acquisition IA Strategy provides documentation that "Ensure that the program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards." The program manager develops the Acquisition IA Strategy to help the program office organize and coordinate its approach to identifying and satisfying IA requirements consistent with DoD policies, standards, and architectures.

The Acquisition IA Strategy serves a purpose separate from the documentation generated from the DIACAP or other Certification and Accreditation (C&A) processes. Developed earlier in the acquisition life cycle and written at a higher level, the Acquisition IA Strategy documents the program's overall IA requirements and approach, including the determination of the appropriate certification and accreditation process. The Acquisition IA Strategy must be available for review at all Acquisition Milestone Decisions, including early milestones when C&A documentation would not yet be available.

The Acquisition IA Strategy lays the groundwork for a successful C&A process by facilitating consensus among the Program Manager, Component Chief Information Officer, and DoD Chief Information Officer on pivotal issues such as Mission Assurance Category, Confidentiality Level, and applicable Baseline IA Controls; selection of the appropriate C&A process;

identification of the Designated Accrediting Authority and Certification Authority; and documenting a rough timeline for the C&A process.

7.5.9.1. Development

Although the development of the Acquisition Information Assurance (IA) Strategy is the responsibility of the program office, a Working-level Integrated Product Team (WIPT) should support the development effort. The WIPT should consist of subject matter experts familiar with the system being acquired, the intended use of the system, and the operational and system architectures within which the system will function. As the operational and system architectures mature, the WIPT should plan for and coordinate interface details with managers of systems and subsystems with which the system being acquired will interface.

The Acquisition IA Strategy is a stand-alone document. Although other key documents can be referenced within the Acquisition IA Strategy to identify supplemental or supporting information, the Acquisition IA Strategy should contain sufficient internal content to clearly communicate the strategy to the reader. If a single document is employed by the program to consolidate acquisition documentation, the Acquisition IA Strategy should be included as a separate section of the document.

Configuration control of the Acquisition IA Strategy should be maintained with respect to the program's governing requirements document (Initial Capabilities Document, etc.) and the Information Support Plan (formerly known as the Command, Control, Communication, Computers, and Intelligence Support Plan). If a governing capabilities document or the Information Support Plan is updated, the Acquisition IA Strategy should be validated or updated accordingly.

The IA Strategy Format Template, while not mandatory, will help you construct an Acquisition IA Strategy document that will satisfy statutory review requirements. Write the document at the unclassified level, and include classified annexes, if required. Factors determining the specific content and level of detail needed can include the following:

- *Acquisition life-cycle stage.* Strategies for programs that are early in the acquisition life cycle will be necessarily at a higher level and less definitive than more mature programs. The level of detail in an Acquisition IA Strategy will increase as a program transitions from one acquisition phase to the next. At program initiation, an IA Strategy is not expected to contain all of the information about initial operating capabilities or future system interfaces that will be available at Milestone B or at the full-rate production decision point. Requirements, employment concepts, and architectures for both the system being acquired, and the systems with which it interfaces, will evolve and mature throughout the acquisition life cycle. As the program matures, the IA Strategy should also evolve. The strategy should be maintained with revisions as required until system retirement and disposal.

- *Extent of system/network interaction.* Systems with a high degree of system-to-system information exchange, or systems connected to the Global Information Grid may require more comprehensive discussions of IA considerations related to their environment.
- *Mission Assurance Category and Confidentiality Level.* Systems with higher mission assurance categories and higher confidentiality levels may require more comprehensive strategies than those with lower levels.
- *Developmental systems versus Commercial-Off-the-Shelf (COTS) Items.* Programs acquiring new systems through development will require more robust treatment of the identification, design, systems engineering and testing of IA requirements than non-developmental programs. Acquisition IA Strategies for the acquisition of COTS systems, however, should also address the approach employed to ensure that the COTS products meet IA requirements and comply with the product specification and evaluation requirements of DoD Instruction 8500.2, Enclosure 3, paragraph E3.2.5.
- *Evolutionary Acquisitions.* Programs employing evolutionary acquisition should differentiate the identification and satisfaction of IA requirements, certification and accreditation activities, and milestone reviews for each increment planned.
- *Special Circumstances.* In the following specific cases, Acquisition IA Strategy content is limited as noted, in consideration of the unique characteristics of these acquisition programs:
    - *Family of Systems Acquisition Programs.* The Acquisition IA Strategy for these programs may be written at a capstone level, focusing on the integration of IA requirements and controls, coordination of System Security boundaries, and ensuring IA resourcing for own and subordinate systems.
    - *Platform IT with interconnection to an external system or network.* In accordance with DoD Instruction 8500.2, Enclosure 3, paragraph E3.4.1.4, the Acquisition IA Strategy must specifically address IA protection for the interconnection points.
    - *Platform IT with no interconnection to an external system or network.* The requirement for an Acquisition IA Strategy can be satisfied by inserting the following statement in the program's Title 40/Clinger-Cohen Act (CCA) Compliance Table submission: "Platform IT does not have an interconnection to an external network." DoD Instruction 5000.02 provides further guidance on the submission of a Title 40/CCA Compliance Table. Although not required, program managers responsible for this type of acquisition would be prudent to consider and implement the IA guidance in DoD Directive 8500.01E and DoD Instruction 8500.2. Click here for more on Title 40/CCA.

DoD Components may require additional questions/areas of concerns (e.g., Critical Infrastructure Protection; Privacy Impact, etc.) in separate DoD Component-specific implementing guidance for Acquisition IA Strategy content and submission.

7.5.9.2. Review Requirements

Acquisition Information Assurance (IA) Strategies must be submitted for approval and review in accordance with Table 7.5.9.2.T1, which is based on submission requirements detailed in DoD

Instruction 5000.02, Enclosures 4 and 5. Sufficient time should be allowed for Acquisition IA Strategy preparation or update, DoD Component Chief Information Officer (CIO) review and approval, and DoD CIO review prior to applicable milestone decisions, program review decisions, or contract awards.

Acquisition Category *	Events requiring prior Review	Acquisition IA Strategy Approval	Acquisition IA Strategy Review
ACAT IAM, IAC, and ID; and (if MAIS) ACAT IC	Milestone A, B, C, full rate production decision and acquisition contract award	Component CIO	DoD CIO
All other acquisitions	Milestone A, B, C, full rate production decision and acquisition contract award	Component CIO or Designee	Delegated to Component CIO

*Acquisition Category (ACAT) descriptions are provided in DoD Instruction 5000.02, Table 1

Table 7.5.9.2.T1. IA Strategy Approval and Review Requirements

7.5.9.3. Additional Information

Questions or recommendations concerning the Acquisition IA Strategy or its preparation or the IA strategy template should be directed to the Defense-wide Information Assurance Program Office (OASD(NII)-DIAP) at diap.acquisition@osd.mil.

7.5.9.4. Acquisition Information Assurance (IA) Strategy Template

(PROGRAM NAME)

1. **Program Category and Life-Cycle Status:** Identify the Acquisition Category (ACAT) of the program. Identify current acquisition life-cycle phase and next milestone decision. Identify whether the system has been designated a "Mission Critical Information System" or "Mission Essential Information System" in accordance with DoD Instruction 5000.02, Enclosure 5. Include a graphic representation of the program's schedule.
2. **Mission Assurance Category (MAC) and Confidentiality Level:** Identify the system's MAC and Confidentiality Level as specified in the applicable capabilities document, or as determined by the system User Representative on behalf of the information owner, in accordance with DoD Instruction 8500.2.
3. **System Description:** Provide a high-level overview of the specific system being acquired. Provide a graphic (block diagram) that shows the major elements/subsystems that make up the system or service being acquired, and how they fit together. Describe the system's function, and summarize significant information exchange requirements and

interfaces with other IT or systems, as well as primary databases supported. Describe, at a high level, the IA technical approach that will secure the system, including any protection to be provided by external systems or infrastructure.

[Note: Programs should engage National Security Agency early in the acquisition process for assistance in developing an IA approach, and in obtaining Information Systems Security Engineering (ISSE) services, to include describing information protection needs, defining and designing system security to meet those needs, and assessing the effectiveness of system security. ISSE efforts are also needed to assess, and if needed, modify the IA component of the system architecture to ensure it is in compliance with the IA component of the Global Information Grid architecture, and makes maximum use of enterprise IA capabilities and services.]

4. **Threat Assessment:** Describe the methodology used to determine threats to the system (such as the System Threat Assessment), and whether the Information Technology (IT) was included in the overall weapon system assessment. In the case of an Automated Information System application, describe whether there were specific threats unique to this system's IT resources due to mission or area of proposed operation. For Major Automated Information System programs, utilization of the "Information Operations Capstone Threat Capabilities Assessment" (DIA Doc # DI-1577-12-03) [1st Edition Aug 03] is required.
5. **Risk Assessment:** (Include as classified annex if appropriate.) Describe the program's planned regimen of risk assessments, including a summary of how any completed risk assessments were conducted.
6. **Information Assurance Requirements:** Describe the program's methodology for addressing IA requirements early in the acquisition life cycle. Identify the applicable sets of Baseline IA Controls from DoD Instruction 8500.2 that will be implemented. Specify whether any specific IA requirements are identified in the approved governing requirements documents (e.g. Capstone Requirements Document, Initial Capabilities Document, Capability Development Document or Capability Production Document). Describe how IA requirements implementation costs (including costs associated with certification and accreditation activities) are included and visible in the overall program budget.
7. **Acquisition Strategy:** Provide a summary of how information assurance is addressed in the program's overall acquisition strategy document. Describe how the Request for Proposal (RFP) for the Engineering and Manufacturing Development Phase contract was, or will be, constructed to include IA requirements in both the operational and system performance specifications, and integrated into the system design, engineering, and testing. In addition, describe how the RFP communicates the requirement for personnel that are trained, and appropriately certified in IA in accordance with DoD Directive 8570.01. Address whether the program will be purchasing commercial off-the-shelf IA or IA-enabled products, and the program's means for verifying that the product specification and evaluation requirements of DoD Instruction 8500.2, Enclosure 3, paragraph E3.2.5 are satisfied. (DoD's implementation of National Security Telecommunications and

Information Systems Security Policy No. 11, "Revised Fact Sheet National Information Assurance Acquisition Policy") will be followed.

8. **Certification and Accreditation:** Identify the specific Certification and Accreditation (C&A) process to be employed (e.g., DoD Information Assurance Certification and Accreditation Process (DIACAP), DoD Information Technology Security Certification and Accreditation Process (DITSCAP), NSA/CSS Information Systems Certification and Accreditation Process (NISCAP), DoD Intelligence Information System (DODIIS)). Effective 28 Nov 07, DIACAP replaced DITSCAP. If using DITSCAP, cite the specific transition authority from DoD Instruction 8510.01 that permits the system to remain under DITSCAP. Provide the name, title, and organization of the Designated Accrediting Authority, Certification Authority, and User Representative. If the program is pursuing an evolutionary acquisition approach, describe how each increment will be subjected to the certification and accreditation process. Provide a timeline graphic depicting the target initiation and completion dates for the C&A process, highlighting the issuance of Interim Authorization to Test (IATT), Interim Authorization to Operate (IATO), and Authorizations to Operate (ATOs). Normally, it is expected that an ATO will be issued prior to operational test and evaluation. If the C&A process has started, identify significant activity completed, and whether an ATO or IATO was issued. If the system being acquired will process, store, or distribute Sensitive Compartmented Information, compliance with Director of Central Intelligence Directive (DCID) 6/3 "Protecting Sensitive Compartmented Information within Information Systems" is required, and the plan for compliance should be addressed.
9. **IA Testing:** Discuss how IA testing has been integrated into the program's test and evaluation planning, and incorporated into program testing documentation, such as the Test and Evaluation Master Plan.
10. **IA Shortfalls:** (Include as classified annex if appropriate) Identify any significant IA shortfalls, and proposed solutions and/or mitigation strategies. Specify the impact of failure to resolve any shortfall in terms of program resources and schedule, inability to achieve threshold performance, and system or warfighter vulnerability. If the solution to an identified shortfall lies outside the control of the program office, provide a recommendation identifying the organization with the responsibility and authority to address the shortfall. If applicable, identify any Acquisition Decision Memoranda that cite IA issues.
11. **Policy/Directives:** List the primary policy guidance employed by the program in preparing and executing the Acquisition IA Strategy, including the DoD 8500 series, and DoD Component, Major Command/Systems Command, or program-specific guidance, as applicable. The Information Assurance Support Environment web site provides an actively maintained list of relevant statutory, Federal/DoD regulatory, and DoD guidance that may be applicable.
12. **Relevant Associated Program Documents:** Provide statement that this version of the Acquisition IA Strategy is reflective of the Program Operational Requirements Document/Initial Capabilities Document/Capability Development Document/Capability Production Document dated _____, and the Information Support Plan (ISP) dated

_____. [Note: Subsequent revisions to the requirements documents or ISP will require a subsequent revision or revalidation of the Acquisition IA Strategy.]

13. **Point of Contact:** Provide the name and contact information for the program management office individual responsible for the Acquisition IA Strategy document. It is recommended that the program office's formally appointed Information Assurance Manager (as defined in DoD Instruction 8500.2) be the point of contact.

7.5.9.5. Information Assurance (IA) Considerations in the Acquisition Strategy

The purpose of including this discussion in the Acquisition Strategy is to clearly convey to the reader of the Acquisition Strategy all IA issues that will impact the acquisition of material or services in support of the system acquisition. It is the means of highlighting to the acquisition team those IA considerations that must be included in solicitations or contracts, or purchased, arranged through supporting memoranda of understanding/agreement, secured through Service Level Agreements, or acquired from another agency via a Military Interdepartmental Purchase Request. In short, it should identify anything IA-related that substantively impacts the program's acquisitions.

The following text is recommended for tailoring as the IA section of an Acquisition Strategy. The presented "considerations" are examples, but experience has shown that they are common to most programs. The program's information assurance manager (IAM) should tailor and augment this template with information drawn from the program's acquisition information assurance strategy.

Template for the IA Section of an Acquisition Strategy

Information Assurance. The _____ PMO has reviewed all appropriate Information Assurance (IA) policy and guidance, and has addressed the implementation of these IA considerations in the _____ Program Information Assurance Strategy, which was approved by the Component CIO on __(date)__. IA requirements, to include the set of DoDI 8500.2 baseline IA controls commensurate with the system's Mission Assurance Category (MAC) and Confidentiality Level, shall be clearly communicated to offerors in the program's solicitations and contracts. IA requirements will be addressed throughout the system life cycle in accordance with DoDD 8500.01E, DoDI 8500.2, and DoDI 8510.01 (DIACAP). [include: "and Director of Central Intelligence Directive 6/3" but only if system handles Sensitive Compartmented Information]. The _____ Program IA Strategy is an integral part of the program's overall acquisition strategy, identifying the technical, schedule, cost, and funding issues associated with executing requirements for information assurance. The following summarizes significant IA considerations impacting the program's acquisition strategy.

IA Technical Considerations. _____ will employ Commercial-Off-The-Shelf (COTS) IA and IA-enabled products as part of the security architecture. These products must be National Security Telecommunications and Information Systems Security Policy Number 11 (NSTISSP-

11) compliant, requiring them to be validated by accredited labs under the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme or National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Cryptographic Module Validation Program (CMVP). Similarly, Government-Off-The-Shelf (GOTS) IA or IA-enabled products employed by the system must be evaluated by the National Security Agency (NSA) or in accordance with NSA-approved processes [and/or other significant technical issues as required].

IA Schedule Considerations. The IA certification and accreditation timeline includes significant events that impact the overall testing, operational assessment and deployment schedules. Key milestones such as issuance of Interim Authorization to Test, Interim Authorization to Operate, and Authorization to Connect, as well as the overall certification and accreditation schedule, are integrated into the program's Test & Evaluation Master Plan (TEMP). [Address other significant schedule issues as required.]

IA Cost Considerations. IA specific costs include Information Systems Security Engineering (ISSE) support, development/procurement, test & evaluation, and certification & accreditation of the IA architecture. It also includes operations and maintenance costs related to maintaining the system security posture following deployment. [Identify any high-impact issues.]

IA Funding Considerations. All IA life-cycle costs are adequately funded. [If not, explain what is not funded and why.]

IA Staffing and Support Issues. The PMO is adequately staffed to support IA requirements, with (X) Government staff assigned full time IA duties. One member of the PMO staff has been appointed Information Assurance Manager for the system, in accordance with DoD Directive 8500.1. Support contractors are required to provide X full-time-equivalents of IA support to the PMO. In addition, [activity X] will provide Certification and Accreditation (C&A) support to the program. [Address other significant staffing and support issues as required.]

7.5.10. Information Assurance (IA) Certification and Accreditation (C&A)

In accordance with DoD Directive 8500.01E, all acquisitions of Automated Information Systems (to include Major Automated Information Systems), outsourced Information Technology-based processes, and platforms or weapon systems with connections to the Global Information Grid must be certified and accredited. The primary methodology for certifying and accrediting DoD information systems is the DoD Information Assurance Certification and Accreditation Process (DIACAP) of DoD Instruction 8510.01.

The previous standard for C&A of non-Sensitive Compartmented Information systems was the "DoD Information Technology Security Certification and Accreditation Process (DITSCAP), DoD Instruction 5200.40. Systems that are currently undergoing C&A utilizing the DITSCAP process must plan for transitioning to the DIACAP.

7.5.11. Software Security Considerations

For the acquisition of software-intensive Information Technology (IT), especially IT used in National Security Systems, Program Managers should consider the significant operational threat posed by the intentional or inadvertent insertion of malicious code.

The Defense Intelligence Agency can perform an analysis to determine foreign ownership, control, and/or influence of vendors bidding for selection to provide information technology, if warranted. If there is sufficient cause for security concerns based on the analysis, the acquiring organization should conduct an independent evaluation of the software.

The Program Manager should identify the software-intensive IT candidates for Defense Intelligence Agency analysis before the Milestone B decision.

7.5.12. Implementing Information Assurance (IA) in the Acquisition of Information Technology (IT) Services

7.5.12. Implementing Information Assurance (IA) in the Acquisition of Information Technology (IT) Services

DoD Instruction 5000.02, Enclosure 9, provides specific policy requirements for "Acquisitions of Services." Enclosure 9 defines Information Technology (IT) Services as "The performance of any work related to IT and the operation of IT, including National Security Systems. This includes outsourced IT-based business processes, outsourced information technology, and outsourced information functions."

Every year the Department acquires a vast array of IT services from the commercial sector, valued in the billions of dollars. These services support, impact, or utilize DoD information systems and networks both on and off the Global Information Grid. Because of this broad scope it is essential that information assurance be carefully considered as a factor in the planning, procurement, and execution of these services.

All acquisitions of IT services, regardless of acquisition of services category, are subject to Title 40/Clinger-Cohen Act, and to the maximum extent practicable, the Federal Acquisition Regulation and Defense Federal Acquisition Regulation Supplement.

Additionally, in accordance with DoD Directive 8500.01E, information assurance requirements shall be identified and included in the design, acquisition, installation, operation, upgrade or replacement of all DoD information systems. This section describes the actions to be taken to ensure that information assurance requirements are met, and IA is appropriately addressed in acquisitions of IT services.

IA considerations are described for the following "Acquisitions of IT Services" areas:

- Acquisition Strategies or Acquisition Plans
- Requests for Proposals (RFPs)
- Source Selection Procedures
- Ordering Guides
- Review and Notification Process

Throughout this section, the services of an "IA professional" are recommended for the development and review of IA elements within acquisition strategies, plans, and procurement documentation. In selecting the appropriate IA professional support, ensure that the individual's IA knowledge and experience are appropriate to the task. Table 7.5.12.T1 suggests appropriate IA workforce categories and levels from the DoD Manual 8570.01-M, "Information Assurance Workforce Improvement Program Manual," for commonly required tasks. See the manual for details of knowledge, experience, and professional certifications required for each category and level.

Task	Suggested DoD 8570.01M Category and Level
Identify IA technical requirements	IA Technical Level II or III depending on scope and complexity
Identify IA policy and procedural requirements	IA Management Level II
Draft IA section of Acquisition Strategy/Plan	IA Management Level II
Draft IA elements of RFP (including SOW/SOO, Section H clause tailoring, CDRL	IA Management Level II
Draft IA section of ordering guide	IA Management Level II
Develop IA Selection Criteria; participate in SSEB (review offerors' proposals)	IA Technical Level III
Review Acquisition documents, RFP, ordering guide	IA Management Level III

Table 7.5.12.T1. Suggested IA workforce categories and levels

7.5.12.1. Acquisition of Information Technology (IT) Services – Information Assurance (IA) Considerations for Acquisition Strategies or Acquisition Plans

The treatment of IA in an acquisition strategy, and/or acquisition plan, for an acquisition of IT services is different than the considerations normally addressed in a classic system acquisition strategy. In the case of a system acquisition, the focus is to ensure IA is implemented in the design, development, test, and production of the system. In the case of an acquisition of IT services, the IA considerations are dependent on the specific nature of the services being acquired.

The scope of potential IT services, and the associated IA considerations, is extremely diverse. Examples of IT services include, but are not limited to:

- On-site hardware maintenance
- Lease of telecommunications lines (fiber or circuits)
- Software development
- Test and evaluation services
- Certification and accreditation support
- Help desk support
- Computing infrastructure operational support
- Network operations and Computer Security support

Note that in some large indefinite delivery/indefinite quantity (IDIQ) IT services contracts, the actual tasks to be performed are not established until an order is placed, and there may be thousands of individual orders placed by hundreds of different ordering activities. In order to properly inform the acquisition planning process, the IA section of the acquisition strategy needs to identify the IA requirements that are relevant to the IT services being acquired, and describe how the acquisition is being conducted to ensure those requirements will be met. As noted above, the scope of these considerations will vary with the nature of the IT services, but the following list provides a good baseline to structure and populate the IA section of the acquisition strategy:

- What broad IA policies and guidance are applicable?
- What IA protections are relevant to the services being acquired?
- Are there any IT components or systems being delivered coincidental to the IT services?
- Is there an IA professional supporting the acquisition team? Has an IA professional contributed to the development of the solicitation?
- Does the solicitation clearly and unambiguously communicate IA requirements to prospective offerors?
- Does the performance work statement, specifications, or statement of objectives meet information assurance requirements as specified in DFARS Subpart 239.71, "Security and Privacy for Computer Systems," paragraph 239.7102-1(a)?

- Is the satisfaction of IA requirements a factor for award? Will an IA professional provide subject matter expert support to the source selection process?
- If an IDIQ contract is considered, what IA requirements are allocated to the basic contract as global requirements, and what IA requirements are allocated to the order level (and the responsibility of the ordering activity to invoke)? Does the ordering guide clearly communicate to requiring activities and the ordering offices their responsibilities with regards to IA?
- Has the solicitation been reviewed by the appropriate level of IA oversight (Designated Accrediting Authority/Program Executive Officer/Systems Command/Major Command/Component Senior Information Assurance Officer)?
- Will the services contractor have access to or control of Government data?
- Will the contractor need to connect to DoD systems or networks?
- Will the contractor need to certify and accredit his information system?
- Will the contractor's personnel be performing roles that require IA training, IA professional certifications, or background investigations in order to comply with DoD IA policy requirements?

7.5.12.2. Acquisition of Information Technology (IT) Services – Information Assurance (IA) Considerations for Requests for Proposals (RFPs)

As with the acquisition strategy, the IA language in the RFP is driven by the characteristics of the IT service requirement. However, regardless of the specifics of the acquisition, the goal of the RFP is to clearly and unambiguously communicate to potential offerors what our IA requirements are, and what we expect from them in terms of compliance and performance.

Identification of IA Policy Requirements

In most cases the IT service contractor will have to comply with fundamental DoD IA policy, such as DoD Directive 8500.01E and DoD Instruction 8500.2, and CJCS Instruction 6510.01E. It is best to identify in the RFP that compliance with these documents is required. For requirements beyond the fundamentals, the nature of the service becomes the driver. If contractor personnel will have IA roles or privileged system access, the requirements of DoD Directive 8570.1 will apply. If the service involves certification and accreditation support, the DoD Information Assurance Certification and Accreditation Process (DIACAP) of DoD Instruction 8510.01 should be cited. Because it would be impractical to identify all the possible permutations of IT services and IA policy in this guidebook, requiring activities should utilize an IA professional to identify all IA requirements relevant to the IT service.

The following contract language is provided as an example that can be tailored as appropriate, and included in Section H (Special Contract Requirements) of the solicitation:

Sample RFP IA Clause

H.XX INFORMATION ASSURANCE (SEP 2007)

It is DoD policy that Information Assurance (IA) requirements shall be identified and included in the design, acquisition, installation, operation, upgrade, or replacement of all DoD information systems. This includes systems and processes developed within the Defense Acquisition System; systems and processes developed at private expense; outsourced business processes supported by private sector information systems; and outsourced information technologies. Information technology services provided under this contract must comply with statutory and regulatory IA policy. The source documents for this policy are:

1. The National Security Act of 1947
2. Title 40/Clinger-Cohen Act
3. National Security Telecommunications and Information Systems Security Policy No. 11, "Revised Fact Sheet National Information Assurance Acquisition Policy" and associated "Frequently Asked Questions"
4. Federal Information Processing Standards
5. DoD Directive 8500.01E, "Information Assurance"
6. DoD Instruction 8500.2, "Information Assurance Implementation"
7. DoD Instruction 8580.1, "Information Assurance in the Defense Acquisition System"
8. DoD Directive 8570.01, "Information Assurance Training, Certification, and Workforce Management"
9. CJCS Instruction 6510.01E, "Information Assurance (IA) and Computer Network Defense (CND)"
10. Defense Acquisition Guidebook – Chapter 7 Acquiring Information Technology and National Security Systems, Section 7.5 Information Assurance
11. DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)"
12. DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997
13. DoD Manual 8510.1-M, "Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual," July 2000
14. DoD Directive 8581.1, "Information Assurance (IA) Policy for Space Systems Used by the Department of Defense"
15. DCI Directive 6/3, "Protecting Sensitive Compartmented Information within Information Systems"

Each proposal, or proposed task order under this contract, will be screened for compliance with applicable IA statutes, policies, and procedures. Specific requirements will be stated in the performance work statement/statement of objectives.

This special contract provision shall be updated by reference for any changes to source documents. Any new laws or policies applicable to IA subsequent to issuance of this contract will be incorporated into the basic contract unilaterally without equitable adjustment to the basic

contract. Any equitable adjustment shall be assessed by individual task orders that may be affected by the change as applicable.

(End of Sample RFP IA Clause)

Performance Work Statement (PWS) or Statement of Objective (SOO). It is in this section that specific IA requirements, functions and tasks should be communicated to the offerors. This may include identification of IA roles to be performed, specific IA controls to be satisfied, specific IA performance criteria (e.g., availability requirements). This section must clearly communicate what needs to be done with regards to IA.

Contract Data Requirements List (CDRL). In this section, identify any IA-related data products that the potential contractor must produce. This may include reports, IA artifacts, or other IA documentation.

Section M: Evaluation Factors for Award. This section contains the evaluation factors and significant subfactors by which offers will be evaluated and the relative importance that the Government places on these evaluation factors and sub-factors. See section 7.5.12.3 for additional guidance.

IA Performance. In situations where IA performance is critical, the RFP may specifically address the impact of non-compliance or lack of IA performance on the part of the contractor. These impacts may include actions such as: documentation of poor performance, rejection of work products/deliverables, denial of network or physical access to non-conforming personnel, reduction of award fees, assessment of liquidated damages, termination of the contract for the convenience of the government, and termination of the contract for default. If IA is a critical element of the service, engage with the Procurement Contracting Officer as early as possible to define these impacts, and to include the appropriate language in the solicitation and resulting contract. The IA professional, PM, and program lead for test and evaluation will identify IA test and evaluation requirements, metrics, success criteria, and how and when best to conduct the IA testing.

7.5.12.3. Acquisition of Information Technology (IT) Services – Information Assurance (IA) Considerations for Source Selection Procedures

Section M of the Uniform Contract format contains the Evaluation Factors for Award. This section contains the evaluation factors and significant sub-factors by which offers will be evaluated and the relative importance that the Government places on these evaluation factors and sub-factors. IA is just one of numerous factors that may be assessed for the purposes of making a contract award decision. It may be a major contributing factor in a best value determination, or it may be a minimum qualification for an award based primarily on cost or price.

The extent to which IA considerations impact the award factors is a direct function of the clear communication and understanding of the potential loss or damage that an IA failure could subject to a system, organization or mission capability. For this reason, an IA professional should be tasked to assess the IA requirement and risks, and to advise the contracting officer accordingly. As appropriate, an IA professional should develop IA related evaluation factors, and participate in the negotiation of relative weightings of these factors. Correspondingly, an IA professional should also be part of the source selection evaluation board to ensure that the IA aspects of offerors' proposals are assessed for technical and functional appropriateness, adequacy, and compliance with requirements.

7.5.12.4. Acquisition of Information Technology (IT) Services – Information Assurance (IA) Considerations for Ordering Guides

In many large IT services contracts, the initial contract award merely establishes the scope of work, pricing, and other global factors, but no specific work is done until separate task orders are established. For these indefinite delivery-indefinite quantity (IDIQ) contracts, the IA considerations can vary widely from order to order. Additionally, orders may be originated from activities separate from the activity that awarded the basic IDIQ contract, even from other agencies. To ensure that IA is appropriately considered in these individual and potentially unique orders, the "ordering guide" for the contract should inform the ordering activities of their responsibilities with regards to IA. Specifically, ordering/requiring activities are responsible to ensure that any order placed for IT services will result in a commitment from the service provider to deliver services that comply with DoD IA policies. To do this, the ordering activity must be aware of what general IA requirements are invoked in the basic contract, and then ensure that individual orders provide specific details, and any supplemental IA requirements that may be needed to achieve policy requirements. For example, the basic contract may invoke DoD Instruction 8500.2 and require "implementation of appropriate baseline IA controls", but the individual order would have to specify the Mission Assurance Category (MAC) and Confidentiality Level relevant to that order.

Finally, since IT services acquisitions must comply with the Title 40/Clinger-Cohen Act which requires a level of assurance that IA compliance is being achieved, it may be appropriate to direct that a hierarchy of IA review and approvals be established based on factors such as dollar value of the individual orders. This will ensure that qualifying orders are reviewed at an oversight level commensurate with their value.

A sample IA section for an ordering guide is provided below. The specific form, structure and content should be driven by the needs of the acquisition, and the example is provided merely to offer a point of departure, and may not be appropriate for a specific acquisition.

Sample IA Section of an Ordering Guide

Section XX. Information Assurance

It is DoD policy that Information Assurance (IA) requirements shall be identified and included in the design, acquisition, installation, operation, upgrade, or replacement of all DoD information systems. This includes systems and processes developed within the Defense Acquisition System; systems and processes developed at private expense; outsourced business processes supported by private sector information systems; and outsourced information technologies. In order to ensure that all services under this contract comply with a uniform set of fundamental IA policies, the basic contract has required contractor compliance with the following statutory and regulatory IA policies:

1. The National Security Act of 1947
2. Title 40/Clinger-Cohen Act
3. National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, "Revised Fact Sheet National Information Assurance Acquisition Policy" and associated "Frequently Asked Questions"
4. Federal Information Processing Standards
5. DoD Directive 8500.01E, "Information Assurance"
6. DoD Instruction 8500.2, "Information Assurance Implementation"
7. DoD Instruction 8580.1, "Information Assurance in the Defense Acquisition System"
8. DoD Directive 8570.01, "Information Assurance Training, Certification, and Workforce Management"
9. CJCS Instruction 6510.01E, "Information Assurance (IA) and Computer Network Defense (CND)"
10. Defense Acquisition Guidebook – Chapter 7 Acquiring Information Technology and National Security Systems, Section 7.5 Information Assurance
11. DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)"
12. DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997
13. DoD 8510.1-M, "Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual," July 2000
14. DoD Directive 8581.1, "Information Assurance (IA) Policy for Space Systems Used by the Department of Defense"
15. DCI Directive 6/3," Protecting Sensitive Compartmented Information Within Information Systems"

Each proposed task order under this contract will be reviewed for compliance with applicable IA statutes, policies, and procedures. Specific requirements will be stated in the task order Performance Work Statement or Statement of Objectives. The requiring activity will review the package to assure that the IA requirements have been identified and included in the design, acquisition, installation, operation, upgrade, or replacement of all DoD information systems.

The requiring activity will provide the Contracting Officer with a validation statement signed at the appropriate level, verifying that all appropriate IA statutory and regulatory requirements are being addressed. The IA validation statement will be executed at the following levels:

Level	Validation Statement Signatory
< $5M	Executed by the relevant System Information Assurance Manager
$5M < $10M	Executed by the relevant System Designated Approving Authority (DAA)
$10M - Major Automated Information System (MAIS) threshold of DoDI 5000.02	Executed by Component Senior Information Assurance Officer (SIAO)
DoDI 5000.02 MAIS threshold and above	Executed by Component CIO

NOTE: All proposed task orders for the acquisition of Mission Critical or Mission Essential IT (as defined in DoD Instruction 5000.02, Enclosures 5) require an approved Acquisition Information Assurance Strategy in accordance with DoD Instruction 8580.1, which will be provided to the ordering officer in lieu of the IA Validation Statement. The Acquisition Information Assurance Strategy should include the deployment of IA controls commensurate with those defined for each of the Mission Assurance Categories (MAC) in accordance with DoD Instruction 8500.2.

All proposed task orders from non-DoD agencies must include an IA Validation Statement executed at an echelon above the ordering activity.

For centrally processed Task Orders, the Central Ordering Office will insure that all IA or IA-enabled IT hardware, firmware, and software components or products incorporated into DoD information systems comply with the evaluation and validation requirements of NSTISSP No. 11. Prior to releasing a Task Order Request for Proposal, the Contracting Officer shall receive an IA Validation Statement and certification of compliance with Title 40/CCA, as required, from the Requiring Office.

For remotely processed task orders (Decentralized Ordering), the requiring activity will insure that all IA or IA-enabled IT hardware, firmware, and software components or products incorporated into DoD information systems comply with the evaluation and validation requirements of NSTISSP No. 11. Prior to releasing a task order Request for Proposal, the Administrative Contracting Officer (ACO) shall receive an IA Validation Statement and certification of compliance with Title 40/CCA, as required, from the Requiring Office. Upon completion of task order award, the ACO will provide the Procurement Contracting Officer (PCO) with a copy of the task order award, IA Validation Statement, and the compliance certification.

The Requiring Office is responsible for providing to the Contracting Officer:

1. Performance Work Statements, Specifications, or Statements of Objectives that meet information assurance requirements as specified in DFARS Subpart 239.71
2. Inspection and acceptance contract requirements

3. A determination as to whether the information technology requires protection against compromising emanations
4. A determination as to whether the information technology being acquired constitutes a "mission critical" or "mission essential" capability as defined in DoD Instruction 5000.02, Enclosures 5
5. If a "mission critical" or "mission essential" system is being acquired, an approved Acquisition Information Assurance Strategy document, approved by the DoD Component Chief Information Officer (CIO) (reference DoD Instruction 8580.1, paragraph 6.4.1)
6. If for an Acquisition Category (ACAT) IAM, IAC, or ID program, an approved Acquisition Information Assurance Strategy document, approved by the DoD Component CIO and formally reviewed by the DoD CIO (reference DoD Instruction 8580.1, paragraph 6.4.2)
7. IA Validation Statement, signed at the appropriate level, verifying that all appropriate IA statutory and regulatory requirements are being addressed
8. Confirmation of compliance with Title 40/CCA, as required
9. Identification of contractor personnel IA certification requirements for individual task orders. IA certification requirements will be specified for those contractor personnel who will be required to perform IA functions for each level within the Technical Category (Chapter 3), and the Management Category (Chapter 4) as defined in DoD Manual 8570.01-M

In addition, all Commercial Off-The-Shelf IA or IA-enabled products incorporated into DoD information systems must comply with the evaluation and validation requirements of NSTISSP No. 11. Such products must be satisfactorily evaluated and validated either prior to purchase or as a condition of purchase. Evidence shall include a vendor's warrant, in their responses to a solicitation and as a condition of the contract, that the vendor's products will be satisfactorily validated within a period of time specified in the solicitation and the contract. Purchase contracts shall specify that product validation will be maintained for updated versions or modifications by subsequent evaluation or through participation in the National IA Partnership Assurance Maintenance Program or the Common Criteria Recognition Arrangement Assurance Maintenance Program.

All military, civilian, and contractor personnel must be provided IA awareness training and education commensurate with their respective IA responsibilities in accordance with DoD Directive 8570.01, "Information Assurance Training, Certification, and Workforce Management."

Ordering Guide provisions shall be updated by reference for any changes to source documents. Any new laws or policies applicable to IA subsequent to issuance of this contract will be incorporated in to the basic contract by bilateral agreement.

(End of Sample IA Section of Ordering Guide)

7.5.12.5. Acquisition of Information Technology (IT) Services –

Information Assurance (IA) Review and Notification Process

Paragraph 5 of Enclosure 9 of DoD Directive 5000.02 includes specific requirements for higher-level review and approval of proposed acquisitions of services. The following IA reviews are required to be conducted in support of the Decision Authority approval process:

- For acquisitions of IT Services estimated at greater than $250M (basic plus all options)
  - DoD Component IA Review of Acquisition Strategy/Acquisition Plan/Request for Proposal (RFP)
- For acquisitions of IT Services estimated at greater than $500M (basic plus all options)
  - DoD Component IA Review of Acquisition Strategy/Acquisition Plan/RFP, and
  - DoD CIO IA ** Review of Acquisition Strategy/Acquisition Plan/RFP, and
  - Notification of cognizant Mission Area Portfolio Manager by OASD(NII)Acquisition prior to RFP release.

For acquisitions of IT services below the $250M threshold, follow Component guidance. For acquisition of IT services related to telecommunications or transport infrastructure, recommend review for IA technical sufficiency by Defense IA/Security Accreditation Working Group (DSAWG) representative.

** Contact the Defense-wide Information Assurance Program (DIAP) Acquisition Team at diap.acquisition@osd.mil to arrange for early coordination reviews and formal reviews.

7.5.13. Information Assurance (IA) Definitions

The following IA-related definitions are provided to assist the reader in understanding IA terminology. Enclosure 2 of DoD Directive 8500.01E and Enclosure 2 of DoD Instruction 8500.2 are another source for IA-related definitions.

Accreditation Decision. An official designation from a Designated Accrediting Authority (DAA), in writing or digitally signed and made visible to the DoD CIO, regarding acceptance of the risk associated with operating a DoD information system and expressed as an Authorization to Operate (ATO), an Interim Authorization to Operate (IATO), an Interim Authorization to Test (IATT), or a Denial of Authorization to Operate (DATO).

Acquisition Program. A directed, funded effort that provides new, improved, or continuing materiel, weapon, or information system or service capability, in response to an approved need.

Authentication. Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Automated Information System (AIS). See DoD Information System.

Availability. Timely, reliable access to data and information services for authorized users.

Certification. A comprehensive validation of actual IA capabilities and services of a DoD information system, made as part of and in support of the DoD Information Assurance Certification and Accreditation Process (DIACAP), to establish compliance with assigned IA Controls based on standardized procedures.

Certifying Authority (CA). The senior official having the authority and responsibility for the certification of information systems governed by a DoD Component IA Program.

Confidentiality. Assurance that information is not disclosed to unauthorized entities or processes.

Confidentiality Level. Applicable to DoD information systems, the confidentiality level is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, Internet, wireless). The Department of Defense has defined three confidentiality levels: classified, sensitive, and public.

Data. Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations, such as characters or analog quantities, to which meaning is or might be assigned.

Designated Accrediting Authority (DAA). Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Approving Authority and Delegated Accrediting Authority.

DoD Information System. The entire infrastructure, organization, personnel, and components for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology-based processes, and platform information technology interconnections.

- **Automated Information System (AIS) Application.** For DoD information assurance purposes, an AIS application is the product or deliverable of an acquisition program such as those described in DoD Directive 5000.1. An AIS application performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition. An AIS application may be a single software application (e.g., Integrated Consumable Items Support); multiple software applications that are related to a single mission (e.g., payroll or fire control); or a combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System, Defense Messaging System). AIS

applications are deployed to enclaves for operations, and have their operational security needs assumed by the enclave.

- **Enclave.** Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced information technology - based processes they support, and derive their security needs from those systems. They provide standard Information Assurance capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, tactical networks, and data processing centers.
- **Outsourced Information Technology (IT)-based Process.** For DoD Information Assurance purposes, an outsourced IT-based process is a general term used to refer to outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services. An outsourced IT-based process performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations.
- **Platform Information Technology (IT) Interconnection.** For DoD Information Assurance purposes, platform IT interconnection refers to network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition and operations. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric. Examples of platform IT interconnections that impose security considerations include communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration and remote upgrade or reconfiguration.

DoD Information Assurance Certification and Accreditation Process (DIACAP). The DoD processes for identifying, implementing, validating, certifying, and managing IA capabilities and services, expressed as IA Controls, and authorizing the operation of DoD information systems in accordance with statutory, Federal and DoD requirements.

DoD Information Technology Security Certification and Accreditation Process (DITSCAP). [Superseded by the DIACAP.] Previously, the standard DoD process for identifying information security requirements, providing security solutions, and managing

information system security activities. All DoD information systems employing the DITSCAP must transition to the DIACAP.

Family of Systems (FoS). A set or arrangement of independent systems that can be arranged or interconnected in various ways to provide different capabilities. The mix of systems can be tailored to provide desired capabilities, dependent on the situation. An example FoS would be an anti-submarine warfare FoS consisting of submarines, surface ships, aircraft, static and mobile sensor systems and additional systems. Although these systems can independently provide militarily useful capabilities, in collaboration they can more fully satisfy a more complex and challenging capability: to detect, localize, track, and engage submarines.

Global Information Grid (GIG). Globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems. The GIG supports all DoD, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical, and business) in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems. Non-GIG Information Technology (IT) is stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network.

The GIG includes any system, equipment, software, or service that meets one or more of the following criteria:

- Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.
- Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.
- Processes data or information for use by other equipment, software, and services.

Information Assurance (IA) Control. An objective IA condition of integrity, availability or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format, i.e., a control number, a control name, control text, and a control class. Specific management, personnel, operational, and technical controls are applied to each DoD information system to achieve an appropriate level of integrity, availability, and confidentiality.

Information Assurance (IA) Product. Product or technology whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control, non-repudiation of data); correct known vulnerabilities; and/or provide layered defense against

various categories of non-authorized or malicious penetrations of information systems or networks. Examples include such products as data/network encryptors, firewalls, and intrusion detection devices.

Information Assurance (IA)-Enabled Information Technology Product. Product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security-enabled messaging systems.

Information. Any communication or representation of knowledge such as facts, data, or opinion in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Technology (IT). Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the DoD Component. For purposes of the preceding sentence, equipment is used by a DoD Component if the equipment is used by the DoD Component directly or is used by a contractor under a contract with the DoD Component that (1) requires the use of such equipment, or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

Integrity. Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Major Automated Information System (MAIS). A DoD acquisition program for an Automated Information System (either as a product or a service) that is either:

- Designated by the MDA as a MAIS; or
- Estimated to exceed:
    - $32 million in fiscal year (FY) 2000 constant dollars for all expenditures, for all increments, regardless of the appropriation or fund source, directly related to the

AIS definition, design, development, and deployment, and incurred in any single fiscal year; or

- $126 million in FY 2000 constant dollars for all expenditures, for all increments, regardless of the appropriation or fund source, directly related to the AIS definition, design, development, and deployment, and incurred from the beginning of the Materiel Solution Analysis Phase through deployment at all sites; or
- $378 million in FY 2000 constant dollars for all expenditures, for all increments, regardless of the appropriation or fund source, directly related to the AIS definition, design, development, deployment, operations and maintenance, and incurred from the beginning of the Materiel Solution Analysis Phase through sustainment for the estimated useful life of the system.

Milestone Decision Authority (MDA). The designated individual with overall responsibility for a program. The Milestone Decision Authority shall have the authority to approve entry of an acquisition program into the next phase of the acquisition process and shall be accountable for cost, schedule, and performance reporting to higher authority, including Congressional reporting.

Mission Assurance Category. Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories:

- **Mission Assurance Category I (MAC I).** Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. Mission Assurance Category I systems require the most stringent protection measures.
- **Mission Assurance Category II (MAC II).** Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. Mission Assurance Category II systems require additional safeguards beyond best practices to ensure assurance.
- **Mission Assurance Category III (MAC III).** Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. Mission Assurance

Category III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices.

Mission Critical (MC) Information System. A system that meets the definitions of "information System" and "national security system," in Title 40/CCA, the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (Note: The designation of mission critical shall be made by a DoD Component Head, a Combatant Commander, or their designee. A financial management IT system shall be considered a mission-critical IT system as defined by the Under Secretary of Defense (Comptroller).) A "Mission-Critical Information Technology System" has the same meaning as a "Mission-Critical Information System." (Source: DoD Instruction 5000.02, Table 8.)

Mission Essential (ME) Information System. A system that meets the definition of "information system" in Title 40/CCA, that the acquiring DoD Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (Note: The designation of mission essential shall be made by a DoD Component Head, a Combatant Commander, or their designee. A financial management IT system shall be considered a mission-essential IT system as defined by the Under Secretary of Defense (Comptroller). A "Mission-Essential Information Technology System" has the same meaning as a "Mission-Essential Information System." (Source: DoD Instruction 5000.02, Table 8.)

National Security System (NSS). Any telecommunications or information system operated by the U.S. Government, the function, operation, or use of which:

- Involves intelligence activities;
- Involves cryptologic activities related to national security;
- Involves command and control of military forces;
- Involves equipment that is an integral part of a weapon or weapons system; or
- Subject to the following limitation, is critical to the direct fulfillment of military or intelligence missions. This does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

Non-repudiation. Assurance that the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

Outsourced Information Technology-based Process. See DoD Information System.

Platform Information Technology Interconnection. See DoD Information System.

Program Manager (PM). The designated individual with responsibility for and authority to accomplish program objectives for development, production, and sustainment to meet the user's

operational needs. The program manager shall be accountable for credible cost, schedule, and performance reporting to the Milestone Decision Authority throughout the life cycle.

User Representative. The individual or organization that represents the user or user community in the definition of information system requirements.

Weapon(s) System. A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency.

7.6. Electromagnetic Spectrum

7.6.1. Electromagnetic (EM) Spectrum Considerations

The Program Manager (PM) must consider the use of the EM spectrum (hereafter referred to as "spectrum") when delivering capability to the warfighter's or business domains. The fundamental questions are:

- Will the system/equipment require access to spectrum to operate as it is intended (e.g., to communicate with other systems; to collect and/or transmit data, to broadcast signals, etc.)?
- Will sufficient spectrum access be available to operate the system/equipment during its life cycle in the intended operational environment?
- Will the system/equipment, including commercial-off-the-shelf systems delivered by the program, radiate EM energy that could be detrimental to other systems or equipment?
- Will the intended operational electromagnetic environment (EME) produce harmful effects to the intended system, even if the proposed system does not radiate EM energy (such as ordnance)?

Ensuring the compatible operation of DoD systems in peace and in times of conflict is becoming increasingly complex and difficult. DoD's demand for spectrum access is increasing as more systems become net-centric and information is pushed to the "tactical edge." In addition, the

EME in which the DoD operates around the globe is becoming more congested as consumer applications that require spectrum are introduced and take hold. System developers can no longer "assume" their systems will be operating in an interference-free frequency band or that a single band will work around the world. Given these circumstances, DoD Instruction 4650.01 states the following as one of spectrum management's core principles: "Pursue spectrum-efficient technologies to support the increasing warfighter demand for spectrum access and encourage development of spectrum-dependent systems that can operate in diverse EMEs."

National and DoD policies and procedures for the management and use of the EM spectrum direct PMs developing spectrum-dependent (S-D) systems/equipment to consider spectrum requirements and Electromagnetic Environmental Effects (E3) control early in the development process. Given the complex environment (both physical and political) in which DoD forces operate, and the potential for worldwide use of capabilities procured for DoD, early and thorough consideration is vitally important. These policies and procedures are intended to ensure the following:

- Permission is obtained from designated authorities of sovereign ("host") nations (including the United States) to use the equipment within their respective borders and near the geographic borders of other countries (within coordination zones);
- Sufficient spectrum will be available in the operational environment during the system/equipment's life cycle; and
- Equipment can operate compatibly with other S-D equipment already in the intended operational environment (electromagnetic compatibility (EMC)).

Because this requires coordination at the national and international levels, getting spectrum advice early helps a PM identify and mitigate spectrum-related risks and successfully deliver capabilities that can be employed in their intended operational environment.

E3 control is concerned with proper design and engineering to minimize the impact of the EME on equipment, systems, and platforms. E3 control applies to the EM interactions of both S-D and non-spectrum-dependent objects within the operational environment. Examples of non-spectrum-dependent objects that could be affected by the EME include all other electrical/electronic systems, are ordnance, personnel, and fuels. The increased dependency on, and competition for, portions of the EM spectrum have increased the likelihood of adverse interactions among sensors, networks, communications, weapons systems, fuels, personnel, and ordnance.

DoD has established procedures, described below, to identify and mitigate spectrum-related risks and to control the E3 impacts on the equipment, systems, and platforms used by our military forces. Spectrum requirements shall be addressed early in acquisition programs (DoD Instruction 4650.01). In accordance with DoD Directive 3222.3, "DoD Electromagnetic Environmental Effects (E3) Program," proper design and engineering techniques to control E3 shall be considered throughout the acquisition process to ensure the successful delivery of operational capabilities to the warfighter.

7.6.2. Mandatory Policies

7.6.2.1. DoD Instruction 5000.02, "Operation of the Defense Acquisition System"

DoD Instruction 5000.02, dated December 8, 2008, references other spectrum-related policies and restates some of the acquisition-related requirements. However, it was published prior to implementation of DoD Instruction 4650.01 and it needs to be revised. In cases of conflicting policy, DoD Instruction 4650.01 takes precedence for spectrum-related requirements.

The current Instruction states:

- For all electromagnetic (EM) spectrum-dependent systems, Program Managers (PMs) must comply with U.S. and host nation spectrum regulations. They shall submit written determinations to the DoD Component Chief Information Officer or equivalent that the EM spectrum necessary to support the operation of the system during its expected life cycle is, or will be, available. These determinations shall be the basis for recommendations provided to the MDA at the milestones defined in Table 3 in Enclosure 4 of DoD Instruction 5000.02.
- Tables 2-1 and 2-2 in Enclosure 4 state the statutory requirement for all developers of systems/equipment that use the EM spectrum in the U.S. and its possessions to submit a DD Form 1494 "Application for Equipment Frequency Allocation" and get Certification of Spectrum Support from the National Telecommunications and Information Administration.

See Section 7.6.3 for requirements at each acquisition milestone.

7.6.2.2. Title 47, Code of Federal Regulations (CFR), Chapter III, Part 300.1

This regulation requires compliance with the National Telecommunications and Information Administration "Manual of Regulations and Procedures for Federal Radio Frequency

Management", and applies to all Federal Agencies that use the electromagnetic spectrum within the United States and its possessions.

7.6.2.3. Office of Management and Budget (OMB) Circular A-11, Section 33.4

This publication contains the requirement to obtain certification by the National Telecommunications and Information Administration that the radio frequency required can be made available before estimates are submitted for the development or procurement of major radio spectrum-dependent communications-electronics systems (including all systems employing satellite techniques) within the United States and U.S. possessions. Additionally, it requires that spectrum be factored into economic analyses of alternatives to the extent practical.

7.6.2.4. DoD Instruction 4650.01, "Policy and Procedures for the Management and Use of the Electromagnetic Spectrum"

This instruction establishes policy and procedures for management and use of the electromagnetic (EM) spectrum and states:

- The EM spectrum is a critical resource, and access to the spectrum is vital to the support of military operations. Proper management and use of the spectrum available to the Department of Defense shall be an integral part of military planning, research, development, testing, and operations involving spectrum-dependent (S-D) systems.
- DoD Components shall comply with U.S. and host nation spectrum regulations and obtain applicable authorizations before operating S-D systems.
- DoD Components shall obtain U.S. Government certification of spectrum support, as required by the National Telecommunications and Information Administration (NTIA) "Manual of Regulations and Procedures for Federal Radio Frequency Management," prior to authorization to operate for experimental testing, developmental testing, or operations of S-D systems in the United States and its possessions. In addition, many host nations require their own certification before providing authorization to operate.
- For all S-D systems, DoD Components shall determine if there will be sufficient spectrum to support operation of the system during its life cycle. In order to affect design and procurement decisions, DoD Components shall:
    - Identify spectrum-related risks as early as possible via spectrum supportability risk assessments (SSRAs).
    - Review these assessments at acquisition milestones.
    - Manage the risks throughout the system's life cycle.
- To facilitate planning, DoD Components shall ensure current and complete technical performance (parametric) data on S-D systems is captured in DoD spectrum management databases.
- In accordance with NTIA "Manual of Regulations and Procedures for Federal Radio Frequency Management," DoD Components shall consider sharing the spectrum with

other Federal agencies and with commercial spectrum users. Sharing of spectrum shall be accomplished:

- Without degradation to the DoD mission.
- In a manner that provides current and future DoD users with sufficient regulatory protection.
- With minimal risk that such sharing will result in loss of access to the spectrum necessary to perform the DoD mission.

In addition, DoD Instruction 4650.01 states that spectrum policy and spectrum management functions shall be guided by the following core principles:

- Ensure the U.S. warfighter has sufficient spectrum access to support military capabilities.
- Support a U.S. spectrum policy that balances national and economic security, with national security as the first priority.
- Use the spectrum as efficiently and effectively as practical to provide the greatest overall benefit to warfighting capability.
- Pursue spectrum-efficient technologies to support the increasing warfighter demand for spectrum access.
- Encourage development of S-D systems that can operate in diverse electromagnetic environments.
- Actively support U.S. policies and interests in international spectrum bodies and in international and bilateral negotiations for spectrum allocation and access.

7.6.2.5. DoD Directive 3222.3, "DoD Electromagnetic Environmental Effects (E3) Program"

This directive establishes policy and responsibilities for the management and implementation of the DoD E3 Program. This program facilitates mutual electromagnetic compatibility and effective E3 control among land, air, sea, and space-based electronic and electrical systems, subsystems, and equipment, and the existing natural and man-made environments.

It states DoD policy that all electrical and electronic systems, subsystems, and equipment, including ordnance containing electrically initiated devices, shall be mutually compatible in their intended electromagnetic environment without causing or suffering unacceptable mission degradation due to E3.

7.6.3. Spectrum Management Integration into the Acquisition Life Cycle

Program Managers (PMs) shall take the following actions to mitigate spectrum-related risks for spectrum-dependent (S-D) equipment, and minimize the electromagnetic environmental effects (E3) on all military forces, equipment, systems, and platforms (both S-D and non S-D). Consideration of these critical elements throughout the acquisition process will help to ensure successful delivery of capability to the warfighter.

The PM shall include the funding to cover spectrum supportability risk assessments (SSRAs), required certification processes, and control of E3 as part of the overall program budget. Section 7.6.4.1 addresses SSRAs; Section 7.6.4.4 addresses E3.

7.6.3.1. Before Milestone A

- Develop initial spectrum and electromagnetic environmental effects (E3) control requirements for the materiel solutions being considered
- Perform initial regulatory spectrum supportability risk assessment (SSRA) to identify and refine spectrum issues. See Section 7.6.4.1 for details.
- For systems that will be operated in the U.S. and its possessions, complete a Stage 1 (Conceptual) Certification of Spectrum Support through the National Telecommunications and Information Administration (NTIA). Contact your sponsoring military department frequency management office for details on the process. The process can take several months, so start as early as practical. See Section 7.6.4.2 for details.

7.6.3.2. Before Milestone B (or before the first Milestone that authorizes contract award)

- Update the spectrum and electromagnetic environmental effects (E3) control requirements and ensure they are addressed in the Capability Development Document.
- Perform initial technical and initial operational spectrum supportability risk assessments (SSRAs) to identify spectrum issues. See Section 7.6.4.1 for details.
- For systems that will be operated in the U.S. and its possessions, complete a Stage 2 (Experimental) Certification of Spectrum Support through the National Telecommunications and Information Administration. Contact your sponsoring military department (MILDEP) frequency management office for details on the process. The process can take several months so start as early as practical. See Section 7.6.4.2 for details.
- For systems that will be operated outside the U.S. and its possessions, initial discussions with host nations should be conducted to determine if there may be significant obstacles to obtaining authorization to operate. MILDEP frequency managers in conjunction with the Joint Staff will assist the Program Manager in initiating discussions with regional combatant command frequency management offices. Discussion should concentrate on host nations where the systems will be permanently deployed.
- Obtain applicable U.S. and/or host nation authorizations before testing spectrum-dependent systems or components.
- Provide initial technical performance data to Defense Information Systems Agency via supporting MILDEP frequency management offices.
- Discuss spectrum and E3 control requirements and any associated issues in the initial Information Support Plan .
- Define, in the Test Evaluation Master Plan (TEMP), those spectrum-related and E3 control requirements that must be tested during Developmental Test and Evaluation and Operational Test and Evaluation. TEMPs shall include, within the scope of critical operational issues and sub-issues, the requirement to demonstrate the effective E3 control of systems, subsystems, and equipment.
- Address SSRA, certification of spectrum support, and E3 control requirements in the Government's Statement of Work, Performance Specifications, and contract data requirements to be provided to the contractor.

7.6.3.3. Before Milestone C

- Update the spectrum and electromagnetic environmental effects (E3) control requirements and ensure they are addressed in the Capability Production Document.
- Perform a detailed regulatory and a detailed technical spectrum supportability risk assessment (SSRA) to ensure all issues have been identified and are being mitigated. See Section 7.6.4.1 for details.
- For systems that will be operated in the U.S. and its possessions, complete a Stage 3 (Developmental) Certification of Spectrum Support through the National Telecommunications and Information Administration. Contact your sponsoring military department (MILDEP) frequency management office for details on the process. The process can take several months so start as early as practical. See Section 7.6.4.2 for details.

- For systems that will be operated overseas, more detailed discussions with host nations may be required to resolve any significant obstacles to obtaining authorization to operate. MILDEP frequency managers in conjunction with the Joint Staff will assist the Program Manager in initiating discussions with regional combatant command frequency management offices. Discussion should concentrate on host nations where the systems will be permanently deployed.
- Obtain applicable U.S. and/or host nation authorizations before testing spectrum-dependent systems or components.
- Provide updated technical performance data to Defense Information Systems Agency via supporting MILDEP frequency management offices.
- Refine the discussion of spectrum and E3 control requirements and any associated issues in the Information Support Plan for record.
- Refine discussion of spectrum-related and E3 control requirements to be tested in the revised Test Evaluation Master Plan.
- Address SSRA, certification of spectrum support, and E3 control requirements in the Government's Statement of Work, Performance Specifications, and contract data requirements to be provided to the contractor.

7.6.3.4. After Milestone C

- Update regulatory, technical, and operational spectrum supportability risk assessments as needed prior to requesting authorization to operate for other than testing. See Section 7.6.4.1 for details.
- For systems that will be operated in the U.S. and its possessions, complete a Stage 4 (Operational) Certification of Spectrum Support through the National Telecommunications and Information Administration prior to requesting authorization to operate for other than testing. The process can take several months so start as early as possible. See Section 7.6.4.2 for details.
- Obtain applicable U.S. and/or host nation authorizations before testing or operating spectrum-dependent systems or components.
- Changes to operational parameters (e.g., tuning range, bandwidth, emission characteristics, antenna gain and/or height, or output power, etc.) or proposed operational locations will likely require additional spectrum certification actions or require additional E3 analysis or tests.
- Continue to provide updated technical performance data to Defense Information Systems Agency via supporting military department frequency management offices.

7.6.3.5. Spectrum and Electromagnetic Environmental Effects (E3) Control Requirements in the Joint Capabilities Integration and Development System

The JCIDS Manual and CJCS Instruction 6212.01 reference other spectrum-related policies and restate some of the requirements. However, they were published prior to implementation of DoD

Instruction 4650.01 and they need revision. In cases of conflicting policy, DoD Instruction 4650.01 takes precedence for spectrum-related requirements.

CJCSM 3170.01 requires the Capability Development Document and Capability Production Document to address spectrum and electromagnetic environmental effects (E3) control. It also requires spectrum requirements be included in the Net-Ready Key Performance Parameter (NR-KPP).

CJCSI 6212.01 includes spectrum and E3 requirements in the NR-KPP under the heading of Supportability Requirements.

Per CJCSI 6212.01, the Joint Staff will use the following assessment criteria when reviewing documents for interoperability:

- If applicable, does the document identify a requirement for spectrum supportability?
- If applicable, does the document address E3?
- If applicable, does the document address host nation approval?
- If applicable, has a DD Form 1494 been submitted to the military department Frequency Management Office?
- Does the document include a spectrum supportability compliance statement or outline a plan to obtain spectrum supportability?
- Does the document address spectrum supportability as a separate requirement in a paragraph?
- Does the document reference the Spectrum Supportability Assessment (SSA)?

Sample Language. The sample statements shown below should be included, as applicable, as THRESHOLD requirements. The first is used to denote compliance with applicable DoD, national, and international spectrum policies and regulations. The second is used to require compatible operation and includes an additional statement for ordnance safety.

Spectrum. *The XXX System will comply with the applicable DoD, National, and International spectrum management policies and regulations. Required performance data will be submitted to the supporting MILDEP Frequency Management Office. (Threshold)*

Electromagnetic Environmental Effects (E3). *The XXX System shall be mutually compatible and operate compatibly in the EME. It shall not be operationally degraded or fail due to exposure to electromagnetic environmental effects, including high intensity radio frequency (HIRF) transmissions or high-altitude electromagnetic pulse (HEMP). All ordnance items shall be integrated into the system in such a manner as to preclude all safety problems and performance degradation when exposed to its operational EME (HERO). (Threshold)*

7.6.3.6. Spectrum and Electromagnetic Environmental Effects (E3) Control Requirements in the Information Support Plan (ISP)

DoD Instruction 4630.8 references other spectrum-related policies and restates some of the requirements. However, it was published prior to implementation of DoD Instruction 4650.01 and it needs revision. In cases of conflicting policy, DoD Instruction 4650.01 takes precedence for spectrum-related requirements.

According to DoD Instruction 4630.8, the ISP must "discuss RF spectrum needs" in Chapter 2 (see details in Section 7.3.6.7.2). Spectrum-related and E3 control issues shall be described in the ISP Chapter 3 (see details in Section 7.3.6.7.3).

7.6.3.7. Spectrum and Electromagnetic Environmental Effects (E3) Control Requirements in the Test and Evaluation Master Plan (TEMP)

Within the TEMP, the critical operational issues for suitability or survivability are usually appropriate to address spectrum and E3 control requirements. The overall goals of the test program with respect to spectrum and E3 control requirements are to ensure that appropriate evaluations are conducted during developmental test and evaluation, and that appropriate assessments are performed during operational test and evaluation. See Section 9.9.3 and Section 9.9.4 for details.

Sample Language. The following are four examples of critical operational issues statements in the TEMP:

- Will the platform/system (or subsystem/equipment) detect the threat in a combat environment at adequate range to allow a successful mission? (Note: In this example, the "combat environment" includes the operational electromagnetic environment (EME).)
- Will the system be safe to operate in a combat environment? (Note: In this example, electromagnetic radiation hazards issues such as hazards of electromagnetic radiation to personnel, ordnance, and volatile materials and fuels can be addressed, as applicable.)
- Can the platform/system (or subsystem/equipment) accomplish its critical missions? (Note: This example determines if the item can function properly without degradation to or from other items in the EME.)
- Is the platform/system (or subsystem/equipment) ready for Joint and, if applicable, Combined operations? (Note: In this example, the item must be evaluated in the projected Joint and, if applicable, Combined operational EME.)

7.6.3.8. Spectrum and Electromagnetic Environmental Effects (E3) Control Requirements in Performance Specifications

Military Standards (MIL-STD) 461 and 464 and Military (MIL-HDBK) 237 provide crucial guidance that, if followed, should preclude E3 problems with the critical systems provided to the warfighter. (Note: MIL-HDBK 237D does not reflect new requirements in DoD Instruction

4650.01, published in January 09, and needs to be revised. DoD Instruction 4650.01 takes precedence.)

Performance specifications should invoke spectrum-related and E3 control requirements. MIL-STD-461, which defines E3 control (emission and susceptibility) requirements for equipment and subsystems, and MIL-STD-464, which defines E3 control requirements for airborne, sea, space, and land platforms/systems, including associated ordnance, can be used as references. Ordnance includes weapons, rockets, explosives, electrically initiated devices, electro-explosive devices, squibs, flares, igniters, explosive bolts, electric primed cartridges, destructive devices, and jet-assisted take-off bottles.

Sample Language. The following examples address E3 control in subsystem/equipment performance specifications:

Electromagnetic Interference (EMI) Control. *The equipment shall comply with the applicable requirements of MIL-STD-461.*

Electromagnetic Interference (EMI) Test. *The equipment shall be tested in accordance with the applicable test procedures of MIL-STD-461.*

As an alternative, the program manger can tailor E3 control requirements from MIL-STD-461 or MIL-STD-464. Both MIL-STD-461 and MIL-STD-464 are interface standards. See section 9.9.4 for testing standards and guidance from Director, Operational Test & Evaluation and from Development Test and Evaluation. See the DoD ASSIST homepage for additional information on Militart specs and standards.

7.6.3.9. Spectrum and Electromagnetic Environmental Effects (E3) Control Requirements in the Statement of Work (SOW)

The following is an example SOW statement to address spectrum and E3 control requirements:

The contractor shall design, develop, integrate, and qualify the system such that it meets its Operational Performance Requirements and the applicable spectrum and E3 control requirements in the system specification. The contractor shall perform analyses, studies, and testing to ensure the system is designed to comply with the applicable DoD, National, and International spectrum management and E3 control policies and regulations. The contractor shall perform inspections, analyses, and tests, as necessary, to verify that the system complies with the applicable DoD, National, and International spectrum management and E3 control policies and regulations. The contractor shall prepare and update spectrum-dependent system technical performance data throughout the development of the system and shall perform sufficient analysis and testing to characterize the equipment, where necessary. The contractor shall establish and support spectrum and E3 control requirements Working-level Integrated Product Team (WIPT) to accomplish these tasks.

7.6.3.10. Spectrum and Electromagnetic Environmental Effects (E3) Control Requirements in the Contract Data Requirements List (CDRL)

The following are examples of data item requirements typically called out for spectrum supportability and E3 control requirements in the CDRL:

- DI-EMCS-80199B EMI [Electromagnetic Interference] Control Procedures
- DI-EMCS-80201B EMI Test Procedures
- DI-EMCS-80200B EMI Test Report
- DI-EMCS-81540A E3 Integration and Analysis Report
- DI-EMCS-81541A E3 Verification Procedures
- DI-EMCS-81542A E3 Verification Report
- DI-MISC-81174 Frequency Allocation Data

7.6.4. Spectrum Supportability Risk Assessments (SSRAs), Certification of Spectrum Support, Authorizations to Operate, and Electromagnetic Environmental Effects (E3) Control Summaries

7.6.4.1. Spectrum Supportability Risk Assessments (SSRAs)

Spectrum-dependent (S-D) system developers shall identify and mitigate regulatory, technical, and operational spectrum supportability risks using suggested tasks in Table 7.6.4.1.T1. DoD

Components' S-D system developers shall increase the detail of these risk assessments as the S-D system's design matures.

S-D system developers shall assess the risk for harmful interference with other S-D systems and/or harmful radiation-related effects. At a minimum, electromagnetic interference (EMI) and electromagnetic compatibility assessments shall be made.

S-D system developers shall manage spectrum supportability risks with other developmental risks through systems engineering processes.

S-D system developers are encouraged to initiate the SSRA in order to help identify regulatory, technical, and operational risks while completing the appropriate stage of certification of spectrum support.

Complex "family of systems" or "system-of-systems" may require more than one SSRA.

Regulatory	
Initial Regulatory Spectrum Supportability Risk Assessment (SSRA) Tasks	• Determine countries for likely operational deployment within each Combatant Commander area of responsibility. • Determine the internationally recognized radio service of all S-D sub-systems. • Identify portions of the system's tuning range supported by each host nation's (HN's) table of frequency allocation. • Determine the relative regulatory status, for example, co-primary or secondary, assigned to the radio service by the HN's table of frequency allocations. • Obtain international comments on U.S. military systems of the same radio service and with similar technical characteristics submitted for HN spectrum certification (available via the DoD Host-Nation Spectrum Worldwide Database Online). • Identify other U.S. military, U.S. civil, and non-U.S. co-band and adjacent-band and harmonically-related systems likely to be co-site or in close proximity by querying DoD system databases or the appropriate National Telecommunications and Information Administration (NTIA) database. • Identify risks and develop recommendations for

	mitigation of regulatory issues.
Detailed Regulatory SSRA Tasks	• Address Military Communications-Electronics Board (MCEB), NTIA and other guidance resulting from the certification of spectrum support process. • Consult with the DoD Component spectrum management office regarding changes to U.S. Federal or civil telecommunication regulations impacting the system's frequency bands. • Determine if the system meets appropriate military, U.S. national, and international spectrum standards for radiated bandwidth and transmitter characteristics. • Quantify the impacts of any changes to U.S. Government or international spectrum regulations or technical sharing criteria. • Identify risks and develop recommendations for mitigation of regulatory issues.
Updated Regulatory SSRA Tasks	• Address MCEB, NTIA and other guidance resulting from the certification of spectrum support process. • Consult with the DoD Component spectrum management office regarding changes to U.S. Federal or civil telecommunication regulations impacting the system's frequency bands. • Identify risks and develop recommendations for mitigation of regulatory issues.
Technical	

Initial Technical SSRA Tasks	• Determine candidate technologies and their technical parameters:
	  ○ Application: fixed, transportable, mobile
	  ○ Host platform (dismounted soldier, airborne, tactical operations center, etc.)
	  ○ Frequency range of operation
	  ○ Required data throughput
	  ○ Receiver selectivity
	  ○ Receiver criteria required for desired operation
	  ○ Required radiated bandwidth
	  ○ Transmitter power output
	  ○ Antenna performance characteristics

	○ Anticipated HNs for deployment • Perform an initial electromagnetic compatibility (EMC) analysis to identify electromagnetic interactions that require further study. The analysis should use, as a minimum, technical parameters for the candidate system and the technical parameters of S-D systems expected to be in the candidate's operational environment. • Evaluate the initial system parameters with respect to U.S. and appropriate international spectrum standards; develop plans to address non-compliant systems. • Identify risks and develop recommendations for mitigation of technical issues.
Detailed Technical SSRA Tasks	• Evaluate system's performance and effect on other S-D system that operates co-frequency or adjacent frequency expected to be found in the intended operational environment. • Determine the acceptable received interference level between the system being analyzed and other spectrum-dependent systems to ensure neither is significantly degraded and that coexistence is feasible. • Use measured performance of the system's receiver, transmitter, antenna, and appropriate propagation models whenever feasible. • Use propagation models developed specifically for mobile communications systems to determine any potential link degradation and blockage due to atmospheric conditions or terrain and building obstructions within intended deployments areas. • Consider overall system performance to include link availability, with and without interference, while taking into account the effects of the environment (e.g., considering path loss, rain attenuation, humidity, climate, temperature, and water and oxygen absorption). • For non-communications systems (radar, passive sensors, etc.), determine the appropriate operational degradation as a function of the level of received environmental and co-site interference. • Quantify intra-platform EMC among co-sited

	emitters and receivers for complex "system-of-systems" platforms in terms of the possibility and influence of: ○ Inter-modulation ○ Transmitter Harmonic Interference ○ Transmitter Spurious Output Interference ○ Transmitter Noise Interference ○ Receiver Desensitization Interference • Compare the measured system parameters with U.S. national and appropriate international spectrum standards. • Generate technical recommendations regarding mitigating potential interference by implementing channelization plans, advanced narrow-beam antennas, (active, spot and contoured-beam, etc.), as well as use of passive radio frequency components (filters, diplexers, couplers, etc.). • Identify risks and develop recommendations for mitigation of technical issues.
Updated Technical SSRA Tasks	• Quantify impact of changes to the operational "signals-in-space" radio frequency parameters to co-site EMC and E3. • Identify risks and develop recommendations for mitigation of technical issues.
Operational	
Initial Operational SSRA Tasks	• Determine the expected complement of S-D systems anticipated to be in the system's operating environment. The system should operate without experiencing or causing interference as part of the DoD response to conventional and non-conventional (disaster relief) missions. • Perform a more extensive EMC analysis quantifying the potential interference between the candidate system and the S-D systems used by other DoD units in the operational environment. Express the results in operational terms, e.g., the frequency-distance separation requirements between a transmitter and a receiver that must be maintained to achieve compatibility. • Identify risks and develop recommendations for mitigation of technical issues.

Updated Operational SSRA Tasks	• Refine the expected complement of S-D systems anticipated to be in the system's operating environments. • Refine the EMC analysis quantifying the mutual interference between the candidate system and the S-D systems used by other DoD units in the operational environment. • Identify risks and develop recommendations for mitigation of technical issues.

Table 7.6.4.1.T1. SSRA Suggested Tasks (from DoDI 4650.01)

7.6.4.2. U.S. Government (USG) and Host Nation (HN) Certification of Spectrum Support

7.6.4.2.1. U.S. Government (USG) Certification of Spectrum Support

Certification of spectrum support shall be obtained as required National Telecommunications and Information Administration (NTIA) "Manual of Regulations and Procedures for Federal Radio Frequency Management" prior to authorization to operate for experimental testing (Stage 2), developmental testing (Stage 3), or operations (Stage 4) of spectrum-dependent (S-D) systems. (See Chapter 10 of NTIA "Manual of Regulations and Procedures for Federal Radio Frequency Management" for descriptions of the Stages of Certification.)

Program Managers shall request certification of spectrum support via the appropriate Service Frequency Management Office using procedures in Chapter 10 of NTIA "Manual of Regulations and Procedures for Federal Radio Frequency Management."

Additionally, as required by OMB Circular A-11, Section 33.4 (see section 7.6.2.3), this certification must be completed prior to submission of cost estimates for development or procurement of major S-D systems and for all space and satellite systems.

Additional coordination is required for satellite systems per NTIA "Manual of Regulations and Procedures for Federal Radio Frequency Management". Information required for requesting either an exemption from the International Telecommunication Union registration or advanced publication, coordination, and notification of a particular space system must be submitted to the NTIA.

7.6.4.2.2. Host Nation (HN) Certification of Spectrum Support

DoD Components shall request HN certification of spectrum support for spectrum-dependent systems using procedures established in Combatant Commander agreements with HNs and by the Military Communications-Electronics Board. Requirements for certification vary by HN.

Program Managers should contact their appropriate Service Frequency Management Office for details on process and procedures.

7.6.4.3. Authorization to Operate (Frequency Assignment)

Frequency assignments are issued by designated authorities of sovereign nations, such as telecommunications agencies within foreign countries, and the National Telecommunications and Information Administration for the United States and its Possessions. Under certain conditions, other designated authorities, such as DoD Area Frequency Coordinators or Unified and Specified Commanders may grant frequency assignments. Equipment that has not been previously granted some level of certification of spectrum support will not normally receive a frequency assignment. Procedures for obtaining frequency assignments, once the equipment, sub-system, or equipment has become operational, are delineated in regulations issued by the Regional and Functional Commands and/or Military Services.

In most cases, the operational frequency assignments are requested and received as a program is being fielded. However, if the Program Manager has implemented guidance received in response to requests for certification of spectrum support and designed the system as described in the performance data provided, system operators have not historically encountered problems in obtaining operational frequency assignments.

Spectrum congestion, competing systems, and interoperability, all can contribute to encountering some operational limitations, such as geographical restrictions or limitations to transmitted power, antenna height and gain, bandwidth or total number of frequencies made available, etc. Certification to operate in a particular frequency band does not guarantee that the requested frequency(ies) will be available to satisfy the system's operational spectrum requirements over its life cycle.

7.6.4.4. Electromagnetic Environmental Effects (E3) Control (DoD Directive 3222.3)

7.6.4.4.1. Objective for Electromagnetic Environmental Effects (E3) Control

The objective of establishing E3 control requirements in the acquisition process is to ensure that DoD equipment, subsystems, and systems are designed to be self-compatible and operate compatibly in the operational electromagnetic environment (EME). To be effective, the Program Manager should establish E3 control requirements early in the acquisition process to ensure compatibility with co-located equipment, subsystems, and equipment, and with the applicable external EME.

7.6.4.4.2. Impacts When Electromagnetic Environmental Effects (E3) Control Is Not Considered

It is critical that all electrical and electronic equipment be designed to be fully compatible in the intended operational electromagnetic environment. The DoD has experience with items developed without adequately addressing E3. Results include poor performance, disrupted communications, reduced radar range, and loss of control of guided weapons. Failure to consider E3 can result in mission failure, damage to high-value assets, and loss of human life. Compounding the problem, there is increased competition for the use of the spectrum by DoD, non-DoD Government, and civilian sector users; and many portions of the electromagnetic spectrum are already congested with spectrum-dependent items. In addition, new platforms/systems and subsystems/equipment are more complex, more sensitive, and often use higher power levels. All of these factors underscore the importance of addressing E3 control requirements early in the acquisition process.

7.6.4.5. Additional Resources

Spectrum management related information is available on the Joint Spectrum Center website. Spectrum compliance is a special interest area on the Acquisition Community Connection website.

7.6.5. Definitions

Key terms pertaining to spectrum supportability and electromagnetic compatibility (EMC) processes are defined below.

Electromagnetic (EM) Spectrum. *Defined in Joint Publication 1-02 as: The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. The terms "electromagnetic spectrum" and "spectrum" shall be synonymous.*

Electromagnetic Compatibility (EMC). *Defined in Joint Publication 1-02 as: The ability of systems, equipment, and devices that utilize the electromagnetic spectrum to operate in their intended operational environments without suffering unacceptable degradation or causing unintentional degradation because of electromagnetic radiation or response. It involves the application of sound electromagnetic spectrum management; system, equipment, and device design configuration that ensures interference-free operation; and clear concepts and doctrines that maximize operational effectiveness.*

Electromagnetic Environment (EME). *Defined in Joint Publication 1-02 as: The resulting product of the power and time distribution, in various frequency ranges, of the radiated or conducted electromagnetic emission levels that may be encountered by a military force, system, or platform when performing its assigned mission in its intended operational environment. It is the sum of electromagnetic interference; electromagnetic pulse; hazards of electromagnetic radiation to personnel, ordnance, and volatile materials; and natural phenomena effects of lightning and precipitation static.*

Electromagnetic Environmental Effects (E3). *Defined in Joint Publication 1-02 as: The impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems, and platforms. It encompasses all electromagnetic disciplines, including electromagnetic compatibility and electromagnetic interference; electromagnetic vulnerability; electromagnetic pulse; electronic protection, hazards of electromagnetic radiation to personnel, ordnance, and volatile materials; and natural phenomena effects of lightning and precipitation static.*

Host Nations (HNs). Defined in Joint Publication 1-02 as: *A nation which receives the forces and/or supplies of allied nations and/or NATO organizations to be located on, to operate in, or to transit through its territory.*

Spectrum Management. Defined in Joint Publication 1-02 as: *Planning, coordinating, and managing joint use of the electromagnetic spectrum through operational, engineering, and administrative procedures. The objective of spectrum management is to enable electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference.*

Spectrum-Dependent Systems. Defined in DoDI 4650.01 as: *All electronic systems, subsystems, devices, and/or equipment that depend on the use of the spectrum to properly accomplish their function(s) without regard to how they were acquired (full acquisition, rapid acquisition, Joint Concept Technology Demonstration, etc.) or procured (commercial off-the-shelf, government off-the-shelf, non-developmental items, etc.).*

Spectrum Supportability Risk Assessment (SSRA). Defined in DoDI 4650.01 as: *Risk assessment performed by DoD Components for all S-D systems to identify risks as early as possible and affect design and procurement decisions. These risks are reviewed at acquisition milestones and are managed throughout the system's life cycle.*

7.7. Accessibility of Electronic and Information Technology

In accordance with Section 508 of Public Law 105-220, "The Workforce Investment Act of 1998," Federal agencies must procure, develop, maintain, or use electronics and Information Technology (IT) that is accessible to people with disabilities. The law further directs the United States Access Board to develop standards to support Section 508. For Program Managers (PMs) who will be acquiring IT, the General Services Administration provides assistance. Included at this site is the Voluntary Product Accessibility Template or VPAT, which helps PMs identify products and vendors that comply with this Federal law.

7.8. The Clinger-Cohen Act (CCA) -- Subtitle III of Title 40 United States Code (U.S.C.)

7.8.1. Overview

Subtitle III of Title 40 of the United States Code (formerly known as Division E of the Clinger-Cohen Act (CCA) (hereinafter referred to as "Title 40/CCA") applies to all Information Technology (IT) investments, including National Security Systems (NSS). Title 40/CCA requires Federal agencies to focus more on the results achieved through its (IT) investments, while streamlining the Federal IT procurement process. Specifically, this Act introduces much more rigor and structure into how agencies approach the selection and management of IT projects.

Title 40/CCA generated a number of significant changes in the roles and responsibilities of various Federal agencies in managing the acquisition of IT/NSS. It elevated oversight responsibility to the Director of the Office of Management and Budget (OMB) and established and gave oversight responsibilities to the departmental Chief Information Officer (CIO). Also, under this Act, the head of each agency is required to implement a process for maximizing the value and assessing and managing the risks of the agency's IT acquisitions.

In DoD, the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) has been designated as the ASD(NII)/DoD CIO with the primary responsibility of providing management and oversight of all Department IT/NSS to ensure the Department's IT systems are interoperable, secure, properly justified, and contribute to mission goals.

The basic requirements of the Title 40/CCA, relating to DoD's acquisition process, have been institutionalized in DoD Instruction 5000.02, "Operation of the Defense Acquisition System;" in particular, Enclosure 5, IT Considerations . The requirements delineated in the Title 40/CCA Compliance Table at Enclosure 5 of DoD Instruction 5000.02 must also be considered and applied to all IT investments, regardless of acquisition category, and tailored commensurate to size, complexity, scope, and risk levels. Table 7.8.1.T1 depicts a summary of Title 40/CCA obligations and authorities.

	Statutory Authority	Regulatory Authority

	40 U.S.C. Subtitle III (aka Clinger-Cohen Act (CCA))	2001 NDAA §811 (P.L. 106-398)	DoDI 5000.02
MDAP	Comply	n/a	Confirm Compliance by Component CIO, then DoD CIO
MAIS	Comply	Confirm* Compliance by DoD CIO	Confirm Compliance by Component CIO, then DoD CIO
All Other	Comply	n/a	Confirm Compliance by Component CIO

* "Certifications" of CCA compliance are no longer required by any statute or regulation.

** Section 811 prohibits Milestone A or B approval or the Full-Deployment Decision Review approval of a Major Automated Information System (MAIS) until the DoD CIO "has determined" that the system is being developed IAW the CCA. "Determine" is replaced here with synonym "confirm."

Table 7.8.1.T1. Summary of Clinger-Cohen Act Compliance Confirmations**

This section assists program managers, program sponsors/domain owners, members of the joint staff, and DoD Component CIO community to understand and comply with Title 40/CCA requirements. Their responsibilities are defined throughout this section and at the IT Community of Practice knowledge center, which also contains a vast array of information pertinent to specific aspects of Title 40/CCA compliance.

7.8.2. Definitions of "information technology" and "National Security System" from Title 40/Clinger-Cohen Act

The term "information technology" with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

The term "National Security System" (NSS) means any telecommunications or information system operated by the United States Government, the function, operation, or use of which, (a) involves intelligence activities; (b) involves cryptologic activities related to national security; (c) involves command and control of military forces; (d) involves equipment that is an integral part of a weapon or weapons system, or (e) is critical to the direct fulfillment of military or intelligence missions.

7.8.3. Mandatory Policies

A comprehensive compilation of Federal laws, OMB and Budget circulars, DoD directives and instructions, and OSD policy memorandums, relevant to all aspects of Title 40/Clinger-Cohen Act (CCA) compliance, is available in the CCA Policy Folder of the Acquisition Community Connection.

The Title 40/CCA Compliance Table, Table 7.8.4.T1, in Section 7.8.4 below, details actions required to comply with Title 40/CCA regulatory requirements, mandatory DoD policy, and the applicable program documentation that can be used to fulfill the requirement. This table emulates the DoD Instruction 5000.02 Title 40/CCA Compliance Table, Table 8, with the addition of columns relating the requirement to applicable milestones and regulatory guidance.

The requirements in this table must be satisfied before milestone approval of any Acquisition Category I (i.e., Major Defense Acquisition Program (MDAP)) and IA (i.e., Major Automated Information System (MAIS) Program) and prior to the award of any contract for the acquisition of a Mission-Critical or Mission-Essential Information Technology (IT) system, at any level.

TAKE NOTE: The requirements delineated in this table must also be considered and applied to all IT investments, regardless of acquisition category, and tailored commensurate to size, complexity, scope, and risk levels.

7.8.4. Title 40/Clinger-Cohen Act (CCA) Compliance Table

Table 7.8.4.T1 is a Title 40/CCA compliance table that includes hyperlinks relative to each compliance area. A brief discussion of each compliance area and hyperlinks to additional pertinent information follow the table. For comprehensive coverage of the Title 40/CCA, including policy documents, best practices, examples, and lessons learned, refer to the CCA Community of Practice website.

Actions Required to Comply With Title 40 U.S.C. Subtitle III	Applicable Program Documentation[1]	Applicable Milestone	Regulatory Requirement
1. Make a determination that the acquisition supports core, priority	ICD Approval	Milestone A	CJCSI 3170.01

functions of the Department. [2]			
2. Establish outcome-based performance measures linked to strategic goals. [2]	ICD, CDD, CPD and APB approval	Milestone A & B	CJCSI 3170.01 DoDI 5000.02
3. Redesign the processes that the system supports to reduce costs, improve effectiveness and maximize the use of COTS technology. [2]	Approval of the ICD, Concept of Operations, AoA, CDD, and CPD	Milestone A & B	CJCSI 3170.01 DoDI 5000.02
4. Determine that no Private Sector or Government source can better support the function. [3]	Acquisition Strategy page XX, para XX AoA page XX	Milestone A	CJCSI 3170.01 DoDI 5000.02
5. Conduct an analysis of alternatives. [3]	AoA	For MAIS: Milestone A & B, & FRPDR (or their equivalent) For non-MAIS: Milestone B or the first Milestone that authorizes contract award	DoDI 5000.02
6. Conduct an economic analysis that includes a calculation of the return on investment; or for non-AIS programs, conduct a Life-cycle Cost Estimate (LCCE). [3]	Program LCCE Program Economic Analysis for MAIS	Milestone A & B	CJCSI 3170.01 DoDI 5000.02
7. Develop clearly established measures and accountability for program progress	Acquisition Strategy page XX APB	Milestone B	DoDI 5000.02
8. Ensure that the acquisition is consistent with the Global Information Grid policies	APB (Net-Ready KPP) ISP (Information Exchange	Milestone A, B & C	CJCSI 6212.01 DoDI 5000.02

and architecture, to include relevant standards	Requirements)		
9. Ensure that the program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards	Acquisition Information Assurance Strategy	Milestone A, B, C, FRPDR or equivalent*****	DoDI 5000.02 DoDD 8580.01
10. Ensure, to the maximum extent practicable, (1) modular contracting has been used, and (2) the program is being implemented in phased, successive increments, each of which meets part of the mission need and delivers measurable benefit, independent of future increments	Acquisition Strategy page XX	Milestone B or the first Milestone that authorizes contract award	DoDI 5000.02
11. Register Mission-Critical and Mission-Essential systems with the DoD CIO [4/5]	DoD IT Portfolio Repository	Milestone B, Update as required	DoDI 5000.02

Title 40/CCA Compliance Table Notes:

1. The system documents/information cited are examples of the most likely but not the only references for the required information. If other references are more appropriate, they may be used in addition to or instead of those cited. Include page(s) and paragraph(s), where appropriate.

2. These requirements are presumed to be satisfied for Weapons Systems with embedded IT and for Command Control Systems that are not themselves IT systems.

3. These actions are also required in order to comply with Section 811 of Public Law 106-398 (Reference (ag)).

4. For NSS, these requirements apply to the extent practicable (Title 40 U.S.C. 11103,

Reference (v)). 5. Definitions: Mission-Critical Information System: A system that meets the definitions of "information system" and "national security system" in the Title 40/CCA (Reference (n)), the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (Note: The designation of mission critical shall be made by a Component Head, a Combatant Commander, or their designee. A financial management IT system shall be considered a mission-critical IT system as defined by the Under Secretary of Defense (Comptroller) (USD(C)).) A "Mission-Critical Information Technology System" has the same meaning as a "Mission-Critical Information System." Mission-Essential Information System: A system that meets the definition of "information system" in Reference (n), that the acquiring Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (Note: The designation of mission essential shall be made by a Component Head, a Combatant Commander, or their designee. A financial management IT system shall be considered a mission-essential IT system as defined by the USD(C).) A "Mission-Essential Information Technology System" has the same meaning as a "Mission-Essential Information System." 5. Only unclassified data may be entered into DoD Information Technology Portfolio Repository. If the information about the system being registered is classified up to SECRET collateral level, the system should be registered with the ASD(NII)/DoD CIO by entering it into the DoD Secret Internet Protocol Router Network IT Registry.

Table 7.8.4.T1. Title 40/CCA Compliance Table, Annotated

7.8.5. Other Title 40/Clinger-Cohen Act (CCA)-Related Legislative Requirements

One other topic not addressed in the Title 40/CCA Compliance Table is the Post Implementation Review (PIR), previously referred to as the Post Deployment Performance Review. See Section 7.9 of this guide for an in-depth discussion of PIR.

7.8.6. Title 40, Subtitle III/Clinger-Cohen Act (CCA) Compliance Requirements

7.8.6. Title 40, Subtitle III/Clinger-Cohen Act (CCA) Compliance Requirements

This section provides an overview of the actions stipulated in the Title 40/CCA Compliance Table, which must be addressed and ultimately lead to confirmation of compliance of a Major Automated Information System (MAIS) or Major Defense Acquisition Program (MDAP) by the DoD Component Chief Information Officer (CIO) and the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))/DoD CIO. The DoD Component Requirements Authority, in conjunction with the Acquisition Community, is accountable for requirements 1 through 5 to the table; the program manager is accountable for requirements 6 through 11.

The program manager shall prepare a table similar to Table 7.8.4.T1, above, to indicate which documents support the Title 40/CCA requirements. DoD Component CIOs shall use those supporting documents to assess and confirm Title 40/CCA compliance. For in-depth coverage of each Title 40/CCA requirement, refer to the CCA Community of Practice as well as the links provided in subsections 7.8.6.1 through 7.8.6.11 and section 7.9.

7.8.6.1. Determining that the Acquisition Supports the Core, Priority Functions of the Department

Overview: This element of the Title 40/Clinger-Cohen Act asks if the function supported by a proposed acquisition is something the Federal government actually needs to perform; i.e., for the Department of Defense, is the function one that we (the Department of Defense and/or its Components) must perform to accomplish the military missions or business processes of the Department?

For Warfare Mission Area and Enterprise Information Environment functions, this question is answered in the Joint Capabilities Integration and Development System (JCIDS) process. Before a functional requirement or new capability enters the acquisition process, the JCIDS process (See the JCIDS Manual) requires the sponsor to conduct a series of analyses. The result of these analyses is reported in an Initial Capabilities Document.

Ideally, these analyses will show that the acquisition supports core/priority functions that should be performed by the Federal Government. Moreover, the analysis should validate and document the rationale supporting the relationship between the Department's mission (i.e., core/priority functions) and the function supported by the acquisition.

Who is Responsible? The Sponsor/Domain Owner with cognizance over the function leads the analysis work as part of the JCIDS processes.

Implementation Guidance: Ensure that the JCIDS analytical work addresses the Title 40/CCA question by establishing the linkage between the mission, the function supported, the capability gap and potential solutions. The following questions should be helpful in determining whether a program supports DoD core functions:

- Does the program support DoD core/primary functions as documented in national strategies and DoD mission and strategy documents like the Quadrennial Defense Review, Strategic Planning Guidance, Joint Operating Concepts, Joint Functional Concepts, Integrated Architectures (as available), the Business Enterprise Architecture, the Universal Joint Task List, mission area statements, or Service mission statements?

7.8.6.2. Establish Outcome-based Performance Measures

Overview: Title 40/Clinger-Cohen Act mandates performance and results-based management in planning and acquiring Information Technology (IT) including National Security Systems (NSS). A key element of performance and results-based management is the establishment of outcome-based performance measures, also known as measures of effectiveness (MOE), for needed capability. MOEs for capabilities needed by the Warfighting and Enterprise Information Environment Mission Areas are developed during a Capabilities-based Assessment (CBA) and recorded in a validated Initial Concept Document. The Business Mission Area identifies outcome-based performance measures during the business case development process and records the approved measures in the business plan.

This section defines measurement terminology, relates it to DoD policy and provides guidance for formulating effective outcome-based performance measures for IT/NSS investments. For clarification, the various uses and DoD definitions of MOEs are provided in the CCA Community of Practice (CoP). Regardless of the term used, the Title 40/CCA states that the respective Service Secretaries shall:

- Establish goals for improving the efficiency and effectiveness of agency operations and, as appropriate, the delivery of services to the agency's customers through the effective use of IT/NSS.
- Ensure that performance measurements are prescribed for IT/NSS programs used by or to be acquired for the executive agency, and that the performance measurements measure how well the IT/NSS supports programs of the executive agency.
- Conduct post-implementation reviews of information systems to validate estimated benefits and document effective management practices for broader use.

In summary, we are obligated to state the desired outcome, develop and deploy the solution, and then measure the extent to which we have achieved the desired outcome. For further discussion, see the Title 40/CCA language in OMB Circular A-11, Part 7, Page 16 of Section 300, Part ID. Additionally, discussions on the statutory basis and regulatory basis for MOEs and their verification are available in the IT-CoP.

Who is Responsible?

- The program Sponsor with cognizance over the function oversees the development of the MOEs during the CBA phase of the Joint Capabilities Integration and Development System (JCIDS) process. The Sponsor ensures that the MOEs are outcome-based standards for the validated capabilities.
    - The Program Manager (PM) must be aware of the MOEs and how they relate to overall program effectiveness, and document these MOEs in the Exhibit 300 that is part of DoD's budget submission to OMB.
- The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) assesses the outcome-based measures in deciding whether to certify Title 40/CCA compliance for ACAT IA programs and recommend Section 801 (2366(a)) (or subsequent defense authorization provision) compliance to the Milestone Decision Authority for ACAT ID programs.

Implementation Guidance: This section is written to help the functional proponent prepare the MOEs and to help the PM understand his/her role in the MOE refinement process. The key to understanding and writing MOEs for IT/NSS investments is to recognize their characteristics and source. Therefore, MOEs should be:

- Written in terms of desired outcomes
- Quantifiable (note that both subjective and objective goals can be quantified)
- Serve as a measure of the degree to which the desired outcome is achieved
- Independent of any solution and should not specify system performance or criteria.

To satisfy the requirement that an MOE be independent of any solution and not specify system performance or criteria, the MOE should be established before the Materiel Solution Analysis phase because the MOEs guide the analysis and selection of alternative solutions leading up to Milestone A. Although the MOE may be refined as a result of the analysis undertaken during this

phase, the source of the initial mission/capability MOE is the functional community. The MOE is the common link between the Initial Capabilities Document (ICD), the Analysis of Alternatives and the benefits realization assessment conducted during a post implementation review (PIR) as described in Section 7.9 of this guide.

As stated in Table 8 of DoD Instruction 5000.02, for a weapon system with embedded IT and for command control systems that are not themselves IT systems, it shall be presumed that the acquisition has outcome-based performance measures linked to strategic goals and that they are likely to be found in a JCIDS document (ICD, Capability Development Document or Capability Production Document). Note however that the presumption exists because the JCIDS requires the development of MOEs. For Title 40/CCA confirmation, approved MOEs are required to be presented to the DoD Component Chief Information Officer.

For further MOE writing guidance, see the Information Technology Community of Practice Measures of Effectiveness Area.

7.8.6.3. Redesigning the Processes that the Acquisition Supports

Overview: This element of the Title 40/Clinger-Cohen Act (CCA) asks if the business process or mission function supported by the proposed acquisition has been designed for optimum effectiveness and efficiency. The Title 40/CCA requires the DoD Component to analyze its mission, and based on the analysis, revise its mission-related processes and administrative processes as appropriate before making significant investments in Information Technology (IT). There are a number of ways to accomplish this requirement but this is known as business process reengineering (BPR) and is used to redesign the way work is done to improve performance in meeting the organization's mission while reducing costs.

To satisfy this requirement, BPR is conducted before entering the acquisition process. However, when the results of the Joint Capabilities Integration and Development System (JCIDS) analysis, including the Analysis of Alternatives (AoA), results in a Commercial-Off-The-Shelf (COTS) enterprise solution, additional BPR is conducted after program initiation, to reengineer an organization's retained processes to match available COTS processes. As stated in Table 8 of DoD Instruction 5000.02, for a weapon system with embedded IT and for command and control systems that are not themselves IT systems, it shall be presumed that the processes that the system supports have been sufficiently redesigned if one of the following conditions exist: (1) the acquisition has a JCIDS document (Initial Capabilities Document, Capability Development Document or Capability Production Document) that has been validated by the Joint Requirements Oversight Council (JROC) or JROC designee, or (2) the Milestone Decision Authority determines that the AoA is sufficient to support the initial Milestone decision."

Who is Responsible?

- The Sponsor/Domain Owner with cognizance over the function with input from the corresponding DoD Component functional sponsor is responsible for BPR.

- The Program Manager should be aware of the results of the BPR process and should use the goals of the reengineered process to shape the acquisition.
- The Office of the Director, Program Analysis and Evaluation (OD/PA&E) assesses an Acquisition Category IAM program's AoA to determine the extent to which BPR has been conducted.
- The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) assesses an Acquisition Category IAM program's AoA to determine whether sufficient BPR has been conducted.

Business Process Reengineering: Benchmarking

Benchmarking is necessary for outcome selection and BPR. The Sponsor/Domain Owner should quantitatively benchmark agency outcome performance against comparable outcomes in the public or private sectors in terms of cost, speed, productivity, and quality of outputs and outcomes.

Benchmarking should occur in conjunction with a BPR implementation well before program initiation. Benchmarking can be broken into four primary phases:

- *Planning Phase:* Identify the product or process to be benchmarked and select the organizations to be used for comparison. Identify the type of benchmark measurements and data to be gathered (both qualitative and quantitative data types). One method to gather data is through a questionnaire to the benchmarking organization that specifically addresses the area being benchmarked.
- *Data Collection and Analysis Phase:* Initiate the planned data collection, and analyze all aspects of the identified best practice or IT innovation to determine variations between the current and proposed products or processes. Compare the information for similarities and differences to identify improvement areas. Use root cause analysis to break the possible performance issues down until the primary cause of the gap is determined. This is where the current performance gap between the two benchmarking partners is determined.
- *Integration Phase:* Communicate the findings; establish goals and targets; and define a plan of action for change. This plan of action is often the key to successful BPR implementation. Qualitative data from a benchmarking analysis is especially valuable for this phase. It aids in working change management issues to bring about positive change.
- *Implementation Phase:* Initiate the plan of action and monitor the results. Continue to monitor the product or process that was benchmarked for improvement. Benchmark the process periodically to ensure the improvement is continuous.

7.8.6.4. Determining That No Private Sector or Other Government Source Can Better Support the Function

Overview: This element of the Title 40/Clinger-Cohen Act (CCA) asks if any private sector or other government source can better support the function. This is commonly referred to as the

"outsourcing determination." The Sponsor/Domain Owner determines that the acquisition MUST be undertaken by DoD because there is no alternative source that can support the function more effectively or at less cost. Note that for weapon systems and for command and control systems, the need to make a determination that no private sector or Government source can better support the function only applies to the maximum extent practicable. As an example, consider that both the DoD and the Department of Homeland Security have common interests. This requirement should be presumed to be satisfied if the acquisition has a Milestone Decision Authority-approved acquisition strategy.

Who is Responsible?

- The Sponsor/Domain Owner with cognizance over the function leads the analysis work as part of the Analysis of Alternatives (AoA) process.
- The PM updates and documents the supporting analysis in the AoA and a summary of the outsourcing decision in the Acquisition Strategy.

7.8.6.5. Analysis of Alternatives (AoA)

Overview: The Office of the Director, Program Analysis and Evaluation (OD/PA&E), provides basic policies and guidance associated with the AoA process. For Acquisition Category ID and IAM programs, OD/PA&E prepares the initial AoA guidance, reviews the AoA analysis plan, and reviews the final analysis products (briefing and report). After the review of the final products, OD/PA&E provides an independent assessment to the Milestone Decision Authority (see DoD Instruction 5000.02, Enclosure 7, paragraph 5). See Section 3.3 of this guidebook for a general description of the AoA and the AoA Study Plan.

7.8.6.6. Economic Analysis (EA) and Life-Cycle Cost (LCC) Estimates

Overview: An EA consists of an LCC and a benefits analysis and is a systematic approach to selecting the most efficient and cost effective strategy for satisfying an agency's need. See Sections 3.6 and 3.7 of this guidebook for detailed EA and LCC estimate guidance.

7.8.6.7. Acquisition Performance Measures

Overview: Acquisition performance measures are clearly established measures and accountability for program progress. The essential acquisition measures are those found in the acquisition program baseline (APB): cost, schedule and performance. See section 2.1 of this guide for detailed APB guidance.

7.8.6.8. The acquisition is consistent with the Global Information Grid (GIG) policies and architecture

Overview: The GIG is the organizing and transforming construct for managing Information Technology for the Department. See Section 7.2.1.2 for detailed guidance on GIG policies and architecture.

7.8.6.9. The program has an Information Assurance (IA) strategy that is consistent with DoD policies, standards and architectures

Overview: IA concerns information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection and reaction capabilities. See Section 7.5 of this guidebook for detailed guidance on IA.

7.8.6.10. Modular Contracting

Overview: Under modular contracting, a system is acquired in successive acquisitions of interoperable increments. The Title 40/Clinger-Cohen Act is concerned with modular contracting to ensure that each increment complies with common or commercially acceptable standards applicable to Information Technology (IT) so that the increments are compatible with the other increments of IT comprising the system.

Who is Responsible?

- The Program Manager is responsible for ensuring that modular contracting principles are adhered to.
- The contracting strategy is addressed in the Acquisition Strategy, which is approved by the Milestone Decision Authority.

Implementation Guidance: See Section 4.5.4 of this guidebook for a discussion of Modular, Open Systems Approach as a systems engineering technique that will support modularity, and Section 39.103 of the Federal Acquisition Regulations for a detailed discussion of Modular Contracting.

7.8.6.11. DoD Information Technology (IT) Portfolio Repository (DITPR)

Overview: The DITPR (requires login) supports the Title 40/Clinger-Cohen Act inventory requirements and the capital planning and investment processes of selection, control, and evaluation. The DITPR contains a comprehensive unclassified inventory of the Department's mission critical and mission essential national security systems and their interfaces. It is web-enabled, requires a Common Access Card (CAC) to obtain access, and requires a user account approved by a DoD Component or DoD IT Portfolio Management (PfM) Mission Area or Domain Sponsor. There is a separate inventory on the Secret Internet Protocol Router Network

(SIPRNET) called the DoD SIPRNET IT Registry, which requires a separate user account to obtain access. DoD Components provide their IT systems inventory data to either DITPR or the DoD SIPRNET IT Registry – there is no overlap between the two repositories. Data is entered into DITPR by one of two means. For the Army, Air Force, Department of the Navy (Navy, US Marine Corps), and the TRICARE Management Activity, data is entered into the DoD Component's IT inventory system and uploaded to DITPR by batch update monthly. All other Components work directly online in DITPR. The applicable policy and procedure document is the DoD Information Technology (IT) Portfolio Repository (DITPR) and DoD SECRET Internet Protocol Router Network (SIPRNET) IT Registry Guidance for 2007-2008, September 6, 2007.

Who is Responsible? The Program Manager is responsible for ensuring the system is registered and should follow applicable DoD Component Chief Information Officer (CIO) procedures and guidance.

DITPR Update Procedure: The DITPR guidance outlines a standard, documented procedure for updating its contents on a monthly basis. The rules, procedures, and protocols for the addition, deletion, and updating of system information are available to users once they are registered. Service and Agency CIOs confirm the completeness of the inventory and the accuracy of the data on the inventory on an annual basis.

Use of the DITPR for Decision Making: The DITPR and the DoD SIPRNET IT Registry are the Department's authoritative inventories of IT systems. They provide senior DoD decision makers a coherent and contextual view of the capabilities and associated system enablers for making resource decisions and a common central repository for IT system information to support the certification processes of the various Investment Review Boards (IRBs) and the Defense Business Systems Management Committee (DBSMC). DITPR provides consistent automated processes across the DoD Components to meet compliance reporting requirements (e.g., Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005 (NDAA), Federal Information Security Act of 2002 (FISMA), E-Authentication, Privacy Act, Privacy Impact Assessments, Social Security Number Reduction, Records Management, and Interoperability). DITPR also enables the Mission Areas and the Components to accomplish IT PfM.

7.8.7. Procedure for Risk-Based Oversight (RBO) Process

7.8.7.1. Background

Since the enactment of the Information Technology Management Reform Act of 1996, currently referred to as the Title 40/Clinger-Cohen Act (CCA), Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer ((ASD(NII)/DoD CIO)) has overseen the Title 40/CCA implementation of acquisition category (ACAT) I/IA weapons and automated information systems in accordance with the provisions of DoD Instruction 5000.02. Under the new risk-based oversight policy, the objective is to make ASD(NII)/DoD CIO oversight of Title 40/CCA compliance the exception.

Further, the risk-based Title 40/CCA compliance oversight enables the ASD(NII)/DoD CIO to identify and implement a cost-effective means for ensuring Title 40/CCA compliance, by providing a decision making framework to help leverage Title 40/CCA oversight responsibility to the DoD Component CIO. In a risk-based oversight model, the DoD Component CIOs oversee programs within their portfolios, commensurate with their demonstrated level of capability across Title 40/CCA compliance areas.

7.8.7.2. Procedures for Title 40/CCA Risk-Based Oversight

These procedures are applicable to all Major Automated Information System (MAIS) programs and Major Defense Acquisition Programs (MDAPs), even those delegated to the DoD Components. Nothing in these procedures takes away or detracts from responsibilities currently described in DoD Instruction 5000.02. What the risk-based oversight process addresses is the manner and level of Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (CIO) and DoD Component CIO involvement in oversight of MAIS and MDAP programs. The process is initiated when the DoD Component Chief Information Officer conducts a self-assessment of Title 40/CCA compliance oversight capability.

7.8.7.3. DoD Component Chief Information Officer (CIO) Self-Assessment Document

This document asks a series of questions related to the implementation of oversight for Title 40/Clinger-Cohen Act (CCA) within DoD Components. The primary audience for this assessment is the DoD Component CIO. These questions were derived from a range of resources, including policy and guidance documents, feedback from a 2004-2005 Title 40/CCA Assessment sponsored by the Office of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)/Deputy CIO (DCIO), and USD(AT&L), and input from DoD personnel across multiple organizations and functions. For further information, see the Risk-Based Oversight for Title 40/Clinger-Cohen Act (CCA) Compliance folder in the Information Technology (IT) Community of Practice.

This document "Sample Self-Assessment file: 7.8.7.5. Self-Assessment of CCA Compliance.doc" asks a series of questions related to the implementation of oversight for Title 40/Clinger-Cohen Act (CCA) within DoD Components. The primary audience for this

assessment is the DoD Component CIO. These questions were derived from a range of resources, including policy and guidance documents, feedback from a 2004-2005 Title 40/CCA Assessment sponsored by the Office of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)/Deputy CIO (DCIO) and USD(AT&L), and input from DoD personnel across multiple organizations and functions.

7.9. Post-Implementation Review (PIR)

7.9.1. Background

The Government Performance and Results Act (GPRA) requires that Federal Agencies compare actual program results with established performance objectives. In addition, Section 11313 of Subtitle III of title 40 of the United States Code (formerly known as Division E of the Clinger-Cohen Act (CCA) (hereinafter referred to as "Title 40/CCA") requires that Federal Agencies ensure that outcome-based performance measurements are prescribed for the Information Technology (including National Security Systems (IT/NSS)) to be acquired and that these performance measurements measure how well the IT/NSS supports the programs of the Agency.

DoD Instruction 5000.02, Tables 2-1 and 2-2, identify this information requirement as a Post-Implementation Review (PIR) and require a PIR for all acquisition program increments at the Full-Rate Production Review/Full-Deployment Decision Review (FRPDR/FDDR). To clarify

this requirement, it is a plan for conducting a PIR that is due at the FRPDR or FDDR. The actual PIR is conducted and a report is generated after Initial Operational Capability and generally before Full Operational Capability. (Refer to section 7.9.5 of this guidebook for specific PIR Implementation Steps.)

The Office of Management and Budget (OMB) in OMB Circular A-130 Chapter 8 paragraph b.1(c and d) prescribe PIR procedures within the capital planning and investment control construct for measuring how well acquired IT supports Federal Agency programs.

7.9.2. Overview

This section provides guidance on how to plan and conduct a Post Implementation Review (PIR) for a capability that has been fielded, and is operational in its intended environment. A PIR verifies the measures of effectiveness (MOEs) of the Initial Capabilities Document (ICD) or the benefits of a business plan, and answers the question, "Did the Service/Agency get what it needed, per the Initial Capabilities Document/Business Plan, and if not, what should be done?

Who is Responsible? The Sponsor is responsible for articulating outcome-based performance measures in the form of measures of effectiveness or benefits and ensuring they are reported in the ICD or Business Plan. The Sponsor is responsible for planning the PIR, gathering data, analyzing the data, and assessing the results. The Program Manager (PM) is responsible for maintaining an integrated program schedule that includes the PIR on behalf of the Sponsor. The PM is also responsible for supporting the Sponsor with respect to execution and reporting of the PIR.

What is a PIR? The PIR is a process that aggregates information needed to successfully evaluate the degree to which a capability has been achieved. Table 7.9.2.T1 represents potential sources of such data. Note that the information sources in this table represent a broad segment of acquisition, administrative, and operational activities.

FOT&E Results	Annual Chief Financial Officer Report
Platform Readiness Assessments	Mission Readiness Reviews
COCOM Exercises	Return on Investment Assessment
User Satisfaction Surveys	War Games
Information Assurance Assessments	Lessons Learned

Table 7.9.2.T1. Potential PIR Information Sources

7.9.3. Post Implementation Review (PIR) Within the Acquisition Framework

A useful way to view a PIR is that it is a doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) assessment. As shown in Figure 7.9.3.F1, the capability based assessment (CBA) (or business case for business systems) defines the need, provides measures of effectiveness, and analyzes the changes that may be needed. The "materiel (M)" contribution to the need enters the defense acquisition framework, which coordinates with the remaining DOTLPF process and arrives at the Full-Rate Production Review/Full-Deployment Decision Review -- the final PIR plan is presented at this time. Following Initial Operational Capability the fielded system is integrated with the changes to process and culture implemented during DOTLPF, and becomes a recognizable and measurable capability. The PIR takes place at this time and informs the DOTLPF, acquisition, and future CBA processes.

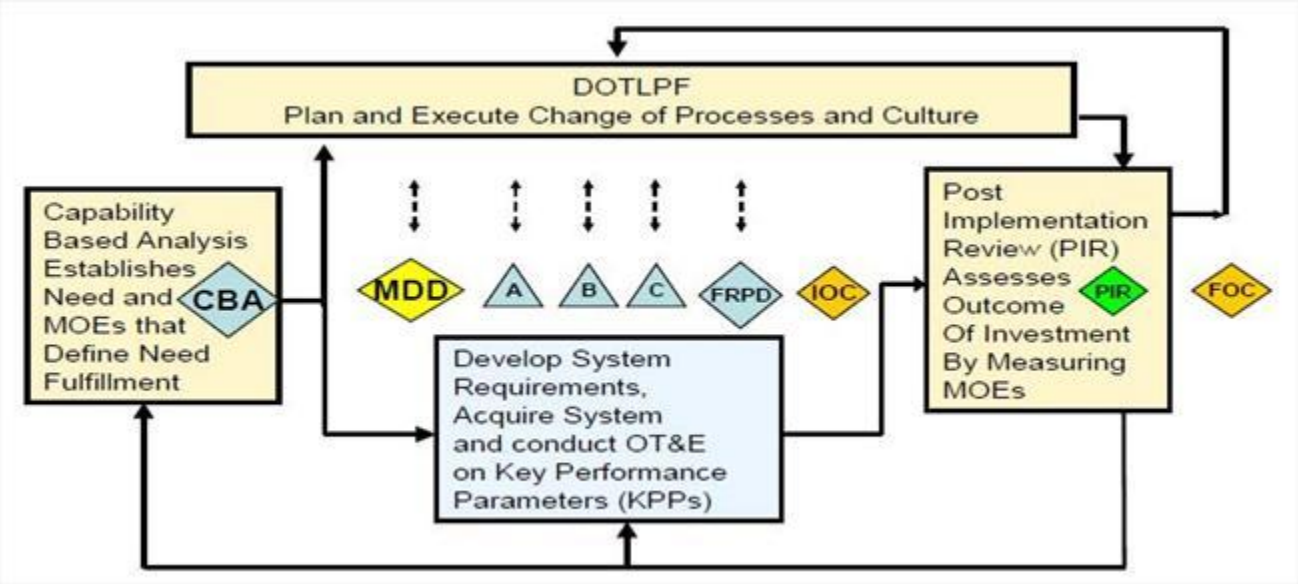


Figure 7.9.3.F1. Identification, Development and Verification of Capability

7.9.4. Post Implementation Review (PIR) Implications for Evolutionary Acquisition

PIRs provide important user feedback and consequently are a fundamental element of evolutionary acquisition. Ideally, we want to understand how well a recently completed increment meets the needs of users before finalizing the requirements for a subsequent increment. In practice however, the opportunity for such feedback depends on the level of concurrency in the increment development schedule.

Additionally, changes in the environment may drive new requirements. The PIR gives both the Sponsor and the Program Manager empirical feedback to better understand any issues with the completed increment. This feedback enables the acquisition principals to adjust or correct the Capability Development Document/Capability Production Document for subsequent increments.

7.9.5. Post Implementation Review (PIR) Implementation Steps

7.9.5.1. Plan the PIR

A draft PIR plan is submitted to the Title 40/Clinger-Cohen Act Action Officer at Milestone B, and a final PIR plan is due at the last acquisition decision review -- Full-Rate Production Review/Full-Deployment Decision Review. When planning the PIR, consider the following:

- Timing of the PIR. The PIR should take place post-Initial Operational Capability after a relatively stable operating environment has been established and the data identified in the PIR plan has been collected. Time frames for the PIR vary with the solution deployment strategy, but generally prior to Full Operational Capability.
- Identification of Scope and Stakeholders
- Team Composition. The PIR team should include, at minimum, the following:
    - Functional experts with working knowledge of the business area and its processes;
    - People with relevant technical knowledge;
    - CIO representatives, functional sponsors, and Domain Owners; and
    - Oversight representatives/
- Identification of information sources. The Initial Capabilities Document or Business Plan that articulated the outcome-based performance measures, or measures of effectiveness (MOEs), is a good place to start. Additional data can be gleaned from operations conducted in wartime and during exercises. The lead-time for most major exercises is typically one year and requires familiarity with the exercise design and funding process. Sources to consider are found in Table 7.9.2.T1.
- Analysis approach. The analysis approach is key to defining the structure and metadata of the information to be collected. For example, the definition of return on investment (ROI) in the Economic Analysis will drive the analysis approach of achieved ROI and the data to be collected.
- Reporting. The report describes the execution of the PIR, addresses the capability gaps that the Information Technology/National Security Systems investment was intended to fill, addresses the degree to which the gaps were filled, and recommends actions to mitigate unfilled capability gaps.
- Resource requirements. Identify the sources of resources such as manpower, travel, analysis tools, communications and other needs unique to the program. Demonstrate agreement by the resource providers; including them in the chop page or citing existing agreements.
- Schedule.

7.9.5.2. Conduct the Post Implementation Review (PIR)

The PIR should be carried out according to the PIR planning that was reviewed and approved at the Full-Rate Production Review/Full-Deployment Decision Review. Care should be given to quality of the raw data. Based on the PIR plan, the PIR should, at a minimum, address:

- Customer Satisfaction: Is the warfighter satisfied that the Information Technology investment meets their needs?
- Mission/Program Impact: Did the implemented capability achieve its intended impact?
- Confirmation that the validated need has not changed; or if it has, include as part of the course of action provided in the PIR report.
- A measure of the measures of effectiveness found in the Initial Capabilities Document.
- Benefits such as return on investment calculations found in the business plan. Compare actual project costs, benefits, risks, and return information against earlier projections. Determine the causes of any differences between planned and actual results.

7.9.5.3. Conduct the Analysis

The analysis portion of the Post Implementation Review (PIR) should answer the question, "Did we get what we needed?" This provides a contrast to the test and evaluation measurements of key performance parameters that answer the question, "Did we get what we asked for?" This would imply, if possible, that the PIR should assess the extent to which the DoD's investment decision-making processes were able to capture the warfighter's initial intent. The PIR should also address, if possible, whether the warfighter's needs changed during the time the system was being acquired. The outputs of the analysis become the PIR findings. The findings should clearly identify the extent to which the warfighters got what they needed.

7.9.5.4. Prepare a Report and Provide Recommendations

Based on the Post Implementation Review (PIR) findings, the PIR team prepares a report and makes recommendations that can be fed back into the capabilities and business needs processes. The primary recipient of the PIR report is the Sponsor who articulated the original objectives and outcome-based performance measures on which the program or investment was based. The results of the PIR can aid in refining requirements for subsequent increments. Recommendations may be made to correct errors, improve user satisfaction, or improve system performance to better match warfighter/business needs. The PIR team should also determine whether different or more appropriate outcome-based performance measures can be developed to enhance the assessment of future spirals or similar IT investment projects.

For further guidance on PIRs, see the Information Technology Community of Practice Post Implementation Review Area. This contains the following additional guidance:

- PIR Measurement Framework
- Common Problems with PIR Implementations
- Example plan and report

7.9.6. Post Implementation Review (PIR) Further Reading

Both government and the commercial sector address the practice of conducting a PIR for materiel, including software and Information Technology, investments. The Government Accountability Office and several not-for-profit organizations have written on the subject of measuring performance and demonstrating results. The Clinger-Cohen Act Community of Practice PIR Area lists a number of key public and private sector resources that can be used in planning and conducting a PIR.

7.9.7. Changes to PIR Guidance Under Development

Section 9.9.10 identifies the intent of the T&E community to: "participate in the planning, execution, analysis, and reporting of PIRs, whose results will be used to confirm the performance of the deployed systems and possibly to improve the test planning and execution for follow-on increments or similar systems." The next iteration of Guidebook section 7.9 will restructure PIR guidance to enable implementation of section 9.9.10.

7.10. Commercial, Off-the-Shelf (COTS) Software Solutions

7.10.1. The Impetus for COTS Software Solutions

One of the Department's goals is to migrate to COTS solutions to fill Information Technology capability gaps.

Subtitle III of Title 40 of the United States Code (formerly known as Division E of the Clinger-Cohen Act (CCA) (referred to as "Title 40/Clinger-Cohen Act") and DoD Instruction 5000.02, Enclosure 2, paragraphs 4.c.(6) and 5.d.(1)(b)3 , all require the use of COTS IT solutions to the maximum practical extent.

7.10.2. Definition

Commercial, Off-the-Shelf (COTS) is defined as "commercial items that require no unique government modifications or maintenance over the life cycle of the product to meet the needs of the procuring agency."

[From the Twelfth Edition of GLOSSARY: Defense Acquisition Acronyms and Terms.]

7.10.3. Mandatory Policies

The following bullets quote or paraphrase sections in the DoD 5000 series that specifically address COTS:

DoD Directive 5000.01, "The Defense Acquisition System" Paragraph E1.1.18, states "…The DoD Components shall work with users to define capability needs that facilitate the following, listed in descending order of preference:

> *"E1.1.18.1. The procurement or modification of commercially available products, services, and technologies, from domestic or international sources, or the development of dual-use technologies; …."*

Hence, commercially available products, services, and technologies are a first priority for acquisition solutions.

DoD Instruction 5000.02, "Operation of the Defense Acquisition System"

- DoD Instruction 5000.02, Enclosure 2, paragraph 4.c.(6), states that "existing commercial off-the-shelf (COTS) functionality and solutions drawn from a diversified range of large and small businesses shall be considered," when conducting the Analysis of Alternatives.
- Enclosure 5, "IT Considerations," Table 8, "Title 40, Subtitle III/CCA Compliance Table," requires that, to be considered Title 40/CCA compliant, the Department must redesign the processes being supported by the system being acquired, to reduce costs, improve effectiveness and maximize the use of COTS technology.
- Enclosure 5, "IT Considerations," Section 8, states that: "When the use of commercial IT is considered viable, maximum leverage of and coordination with the DoD Enterprise Software Initiative shall be made."

7.10.4. COTS Software--Reuse Custom Components

Modifying the core code of a COTS product should be avoided. It is possible to add code to the existing product, to make the product operate in a way it was not intended to do "out-of-the-box." This, however, significantly increases program and total life-cycle costs, and turns a commercial product into a DoD-unique product. The business processes inherent in the COTS product should be adopted, not adapted, by the organization implementing the product. Adopting a COTS product is done through business process reengineering (BPR). This means the organization changes its processes to accommodate the software, not vice versa. In many cases there will be a few instances where BPR is not possible. For example, due to policy or law, it may be necessary to build or acquire needed reports, interfaces, conversions, and extensions. In these cases, adding to the product must be done under strong configuration control. In cases where a particular COTS product does not provide the entire set of required functionality, a "bolt-on" could be used. A bolt-on is not part of the COTS software product, but is typically part of a suite of software that has been certified to work with the product to provide the necessary additional functionality. These suites of software are integrated to provide the full set of needed functionality. Using a bolt-on, however, also increases program and total life-cycle costs.

See section 7.10.6.3 for a more detailed discussion of reports, interfaces, conversions, and extensions.

7.10.5. COTS Integration into the Acquisition Life Cycle

The actions below are unique to acquiring COTS Information Technology solutions. These activities should occur within a tailored, responsive, and innovative program structure authorized by DoD Instruction 5000.02. The stakeholder primarily responsible for each action is shown at the end of each bullet.

7.10.5.1. Before Milestone A

- Define strategy and plan for conducting BPR during COTS software implementation phase of the program.
  (Sponsor/Domain Owner)
- Consider COTS and BPR when developing the Analysis of Alternatives. (See section 3.3 and Table 7.8.4.T1 of this guidebook).
  (Sponsor/Domain Owner)
- Consider commercially available products, services, and technologies when defining initial user needs in the Initial Capabilities Document.
  (Sponsor/Domain Owner)
- When developing the Technology Development Strategy and/or the Acquisition Strategy , consider commercial best practice approaches and address the rationale for acquiring COTS.
  (Program Manager (PM))
- Consider the Initiation and Acquisition best practices available in the Enterprise Integration Toolkit when contracting for the COTS product and the system integrator (if required).
  (Sponsor/Domain Owner and PM)

7.10.5.2. Before Milestone B

- To the maximum extent possible, redesign business processes to conform to the best practice business rules inherent in the COTS product. Define a process for managing and/or approving the development of reports, interfaces, conversions, and extensions. (See the Enterprise Integration Toolkit for best practices in the methodologies and techniques to be successful in this phase.)
  (Sponsor/Domain Owner and Program Manager (PM))
- Consider the Implementation, Preparation, and Blueprinting best practices available in the Enterprise Integration Toolkit.
  Sponsor/Domain Owner and PM)

7.10.5.3. Before Milestone C or Full Rate Production Decision/Full Deployment Decision Review

- Ensure scope and requirements are strictly managed and additional reports, interfaces, conversions, and extensions objects are not developed without prior authorization.
  (Program Manager (PM))
- Consider best practices in the Enterprise Integration Toolkit regarding the implementation phase of the COTS effort.
  (PM)
- Ensure adequate planning for life-cycle support of the program. See section 3.4, Engineering for life-cycle support, of "Commercial Item Acquisition: Considerations and Lessons Learned".

7.10.5.4. After Milestone C or Full-Rate Production Decision/Full-Deployment Decision Review

Conduct ongoing engineering and integration for sustainment activities throughout the life cycle of the program.

7.10.6. Best Practices, Tools, and Methods

Various methodologies, toolsets, and information repositories have been developed to assist the Program Manager (PM) in the implementation of COTS software-based programs. The remainder of this section provides the PM descriptions of best practices, available tools and methods, and critical success factors for use in the acquisition of commercially-based solutions. Additionally, Chapter 4 of this Guidebook, Systems Engineering, presents a complete discussion of applicable systems engineering practices, to include a discussion of the Modular, Open Systems Approach .

7.10.6.1. DoD Enterprise Software Initiative

The DoD Enterprise Software Initiative (DoD ESI) is a joint, Chief Information Officer (CIO)-sponsored project designed to: "Lead in the establishment and management of enterprise COTS information technology (IT) agreements, assets, and policies for the purpose of lowering total cost of ownership across the DoD, Coast Guard and Intelligence communities." DoD ESI is a key advisor to the DoD Strategic Sourcing Directors Board. With active working members from OSD, Department of the Army, Department of the Navy, Department of the Air Force, Defense Logistics Agency, Defense Information Systems Agency, National Geospatial-Intelligence Agency, Defense Intelligence Agency, Director of National Intelligence, and Defense Finance and Accounting Service, the DoD ESI team collaborates to create Enterprise Software Agreements (ESA) for use by DoD, the Intelligence Community, and U.S. Coast Guard IT buyers. ESA negotiations and management activities are performed by IT acquisition professionals within participating DoD Components, who are designated ESI "Software Product Managers (SPM)." SPM are supported by experienced IT contracting experts.

The DoD ESI can use the Defense Working Capital Fund to provide "up-front money" for initial wholesale software buys and multi-year financing for DoD customers. This funding process assures maximum leverage of the combined buying power of the Department of Defense, producing large software discounts.

On-line resources include the DoD ESI website listing general products, services and procedures; the Defense Federal Acquisition Regulation Supplement Subpart 208.74; DoD Instruction 5000.2, Enclosure 5, Paragraph 6 and DoD Component requirements for compliance with DoD Enterprise Software Initiative policies.

The former DoD Business Initiative Council (BIC) endorsed Enterprise Software Initiative operations through BIC Initiative IT01. BIC Initiative IT11 extended Software Asset Management to the DoD Component level and authorized DoD ESI to develop agreements for IT hardware and selected services.

7.10.6.2. SmartBUY

SmartBUY is a federal government strategic sourcing initiative intended to support effective enterprise level software management and achieve government-wide cost avoidance through aggregate buying of commercial software. Besides providing reduced prices and more favorable terms/conditions, the SmartBUY program assists agencies to achieve greater standardization, improved configuration management, and more robust Information Technology security.

The General Services Administration (GSA) manages the SmartBUY Program, and leads the interagency team in negotiating government-wide enterprise licenses for software. The GSA SmartBUY Program focuses on commercial-off-the-shelf software that is generally acquired using license agreements with terms and prices that vary based on volume. The GSA SmartBUY Program was formally announced on June 2, 2003 in an Office of Management and Budget Memorandum to the federal agencies. The DoD ESI Team has worked closely with the SmartBUY project since its inception, and negotiates and manages many of the SmartBUY agreements as a partner to GSA.

The DoD ESI team implements SmartBUY within the DoD through the joint DoD Deputy CIO and DPAP Policy Memorandum of December 22, 2005: Department of Defense (DoD) Support to the SmartBUY Initiative. This policy mandates use of SmartBUY agreements when user requirements match a product on SmartBUY, and also provides the framework for migrating existing Enterprise Software Initiative Enterprise Agreements to SmartBUY Enterprise Agreements. The OMB Memo establishes requirements to be followed by federal departments and agencies. Specifically, federal agencies are to: develop a migration strategy and take contractual actions as needed to move to the government-wide license agreements as quickly as practicable; and integrate agency common desktop and server software licenses under the leadership of the SmartBUY team. This includes, to the maximum extent feasible, refraining from renewing or entering into new license agreements without prior consultation with, and consideration of the views of, the SmartBUY team.

The Federal Acquisition Regulation (FAR) Committee has developed draft regulations to implement SmartBUY.

7.10.6.3. Enterprise Integration Toolkit

The Enterprise Integration Toolkit provides Program Managers (PMs) with a repeatable Commercial-off-the-shelf (COTS) implementation process, a knowledge repository that incorporates both government and commercial industry best practices and lessons learned, and a

Reports, Interfaces, Conversions, and Extensions (RICE) Repository. The objectives of the Enterprise Integration Toolkit are to assure cost savings within the program, to achieve program speed and efficiency, and to reduce program risk. A user ID and password is required and may be obtained by registering at the website.

The Toolkit is the single point of reference for COTS program product examples and templates, and contains a repository of Education & Training courses and lessons learned. PMs should use the Enterprise Integration Toolkit to leverage proven approaches and lessons learned in the areas of program initiation, software and system integration services sourcing, contracting, implementation, education and training, information assurance/security, performance metrics and change management. The Toolkit enables PMs to leverage work already done, and to reduce the redundancy, effort, and costs associated with a COTS implementation. (Education & Training represents a significant portion of COTS implementation costs.)

The Enterprise Integration Toolkit also contains a repository of RICE development objects to be used by PMs to leverage work already done, and to reduce redundancy, effort, and costs of COTS implementations. RICE objects represent a significant portion of COTS cost, not only in the initial development, but in on-going maintenance and updating.

During a COTS implementation, there are additional configuration, design, and/or programming requirements necessary to satisfy functional requirements and achieve the desired functionality. These requirements are not supported within the commercial, core functionality of the COTS product being implemented, and therefore require additional technical development. RICE objects represent the solution to these additional requirements. This development (or reuse) of RICE objects enables the creation of unique Reports not standard in the product; the creation of Interfaces to external systems; the creation of Conversion programs to transfer data from an obsolete system to the new system; and the creation of Enhancements (or Extensions) to allow additional functionality to be added to the system without disturbing the core software code.

To ensure consistency across programs and within the RICE Repository, RICE is further defined as follows:

- **Report** - A formatted and organized presentation of data,
- **Interface** - A boundary across which two independent systems meet and act on or communicate with each other.
- **Conversion** - A process that transfers or copies data from an existing system to load production systems.
- **Extension** - A program that is in addition to an exiting standard program but that does not change core code or objects.

The Enterprise Integration Toolkit also includes a RICE Repository Concept of Operations that provides PMs with a process for leveraging the value of the RICE Repository. This process describes how to take data from and how to provide data to the repository. It describes the timing

for the use of the repository, and at what point and level approvals (Process Owner, PM, Project Sponsor, and Domain Owner) are to be obtained throughout the life cycle of a program.

PMs should ensure vendors include these repositories in their implementation methodologies. The Enterprise Integration Toolkit's software and systems integration acquisition and contracting processes contain boilerplate language for PMs to use in acquisition documents.

For more detail or additional definitions, to review the CONOPS, or to download other material go to the Enterprise Integration Toolkit.

7.10.6.4. Commercial, Off-the-shelf (COTS) Testing

On June 16, 2003, the Director, Operational Test and Evaluation, signed a memorandum issuing the "Guidelines for Conducting Operational Test and Evaluation (OT&E) for Software-Intensive System Increments." The guidelines help streamline and simplify COTS software testing procedures. They assist in tailoring pre-deployment test events to the operational risk of a specific system increment acquired under OSD oversight. For increments that are of insignificant to moderate risk, these guidelines streamline the operational test and evaluation process by potentially reducing the degree of testing. Simple questions characterize the risk and environment upon which to base test decisions, for example, "If the increment is primarily COTS, or government off-the-shelf items, what is the past performance and reliability?"

7.10.6.5. Emerging Information Technology (IT) Market Research and Commercial, Off-the-shelf (COTS) IT Lessons Learned

Section 881 of the FY 2008 National Defense Authorization Act (NDAA) requires the Department to have a Clearing-House for Rapid Identification and Dissemination of Commercial Information Technologies. To meet this need, a partnership between the Under Secretary of Defense (USD) for Acquisition, Technology and Logistics (AT&L), the Director of Defense Research and Engineering (DDR&E), the Defense Technical Information Center (DTIC) and the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) was formed to develop a capability that 1) allows better visibility into the Department's technology needs, 2) attracts non-traditional defense emerging technology suppliers, and 3) allows for review and discussion of COTS IT products in wide use throughout the Department. This effort, termed "DoD Techipedia" will be comprised of both an internal, DoD CAC-only Wiki-based collaboration area, and an external Wiki (internal.dodtechipedia.mil or a separate redirected .mil site) where DoD Capability buyers and their representatives can collaborate with Industry on a range of technology areas. Regarding wide-use COTS IT products, the objective is to raise the awareness of Government and commercial sector practices relative to the use of COTS software. The Enterprise Integration Toolkit contains a section on lessons learned.

DEFENSE ACQUISITION GUIDEBOOK
Chapter 8 -- Intelligence, Counterintelligence, and Security Support

8.0. Overview

8.0.1. Purpose

The purpose of this chapter is three-fold:

1. Focus Program Manager (PM) attention on and describe PM responsibilities regarding the prevention of inadvertent technology transfer of dual-use and leading edge military technologies that support future defense platforms.
2. Inform the PM of the intelligence, counterintelligence (CI), and security support available to, and required for, their program; and,
3. Provide guidance and describe support available for protecting those technologies.

8.0.2. Contents

This Chapter is divided into six sections as follows:

Section 8.0, Overview, provides the purpose of this chapter, briefly summarizes the content and organization, and provides a brief discussion on applicability.

Section 8.1, Introduction, provides an overview of protection considerations, and addresses the planning, legal issues, and information reporting associated with the DoD Research and Technology Protection (RTP) effort.

Section 8.2, Intelligence, contains information on intelligence support to acquisition programs and intelligence supportability.

Section 8.3, Pre-Acquisition Protection Strategy for Research, Development, Test and Evaluation (RDT&E) Activities, covers procedures for RTP at RDT&E facilities.

Section 8.4, Acquisition Protection Strategy for Program Managers, contains procedures for protecting acquisition program technologies and information.

Section 8.5, Specialized Protection Processes, describes procedures in system security engineering, counterintelligence, anti-tamper, information assurance, horizontal analysis and protection, and Research and Technology Protection (RTP) assessments and inspections that apply to protection activities, both at Research, Development, Test and Evaluation (RDT&E) sites and within acquisition programs.

8.0.3. Applicability

This chapter describes procedures for identifying and protecting DoD research and technology selected during research, development, or acquisition as critical program information (CPI), in accordance with DoD Directive 5000.01, DoD Instruction 5000.02, DoD Instruction 5200.39, and DoD 5200.1-M. Criteria for and a definition of CPI is provided in DoD Instruction 5200.39 and in section 8.1.1.

The guidance applies to all activities, phases, and locations (to include contractor locations) where CPI are developed, produced, analyzed, maintained, employed, transported, stored, or used in training, as well as during its disposal.

This Chapter does not apply to acquisitions by the DoD Components that involve a Special Access Program (SAP) created under the authority of Executive Order 12958. The unique nature of SAPs requires compliance with special security procedures of DoD Directive 5205.07. If the program or system contains CPI, the SAP Program Manager will prepare and implement a Program Protection Plan (PPP) prior to transitioning to collateral or unclassified status. Security, intelligence, and counterintelligence organizations should assist the SAP Program Manager in developing the PPP. The PPP will be provided to the offices responsible for implementing protection requirements before beginning the transition.

8.0.4. Acquisition Documents Discussed in Chapter 8

The acquisition program documents discussed in Chapter 8 are listed below in Table 8.0.4.T1. This table lists the documents that are prepared when the program manager or Research, Development, Test and Evaluation (RDT&E) site director determines they are necessary, and includes identification of and electronic links to the sections of Chapter 8 that contain the guidance for the preparation of each document.

Document	Prepare if:	Discussion on Preparation
Program Protection Plan (PPP)	The acquisition program has CPI	8.4.6 DoDI 5200.39
Technology Assessment/Control Plan (TA/CP)	The acquisition program may have, or will have, foreign participation	8.4.3 DoDD 5530.3 DoDD 5230.11
Capstone Threat Assessment (CTA)	During capability shortfall process obtain threat intelligence from CTA	JCIDS Manual
System Threat Assessment Report (STAR) / System Threat Assessment (STA)	Task the supporting intelligence production center prior to MS B; MAIS programs are to use the Information Operations Capstone Threat Assessment	DoDD 5000.02 E4, Table 3 DIAD 5000.200 "Available through the Office of the Director, Defense Intelligence Agency, (703) 695-7353" DIAI 5000.002 "Available through the Office of the Deputy Director for Analysis, Defense Intelligence Agency, (202) 231-4855"
Delegation of Disclosure Authority Letter (DDL)	The acquisition program has foreign participation	8.4.8.3

and Program Security Instruction		DoDD 5530.3 DoDD 5230.11
Counterintelligence Support Plan (CISP)	- For all major Research, Development, Test and Evaluation activities and - For an research, development and acquisition program with CPI - Cleared defense Contractors where research, development and acquisition program CPI is resident	8.3.1.2 8.3.2.1 8.3.4 8.5.2
Counterintelligence (CI) Analysis of CPI	The program has CPI; the CI supporting organization will complete CI analysis and provide an analytical product to the requesting office. A Technology Targeting Risk Assessment (TTRA) may be integrated with or accompany the CI analytical product	8.4.6.2 8.4.7
Life-cycle Signature Support Plan (LSSP)	Acquisition program is signature-dependent	DoDD 5250.01
Security Classification Guide (SCG)	The program contains classified information or controlled unclassified information	8.4.6.5 DoD 5200.1-R
System Security Authorization Agreement (SSAA)	The Information Systems (including network enclaves) is used for storing, processing, or transmitting CPI. Additional information of the SSAA can be found in section 7.5.12 under Information Assurance	8.5.4
System Security Management Plan (SSMP)	The program manager (PM) chooses to use a SSMP to plan the program's system security effort	8.5.1.1 8.5.1.2

Anti-Tamper (AT) Plan	AT measures are applied	8.5.3.3 8.5.3.1
Information Exchange Agreements	The acquisition program has foreign participation	8.3.2.2 8.4.3
Program Protection Implementation plan (PPIP)	The Program Manager (PM) decides to use a PPIP as part of the contract	8.4.9.3
DD Form 254, DoD Contract Security Classification Specification	When the PM includes security controls within the contract or the contract will involve classified information.	8.4.9.7 DoD 5220.22-M

Table 8.0.4.T1. Acquisition Documents Discussed in Chapter 8

8.0.5. Support from Functional Offices

To properly accomplish activities described in this chapter, the Program Manager (PM) needs the cooperation and support of related functional offices. Support to the acquisition community from the intelligence, counterintelligence (CI), and security communities involves a number of staff organizations and support activities that may be unfamiliar to members of the acquisition community. Table 8.0.5.T1 lists the functional offices that may support the PM in various tasks discussed in Chapter 8. This table identifies (and links to) the sections of Chapter 8 that describe various situations involving these offices. The individual assigned responsibility for coordinating intelligence support, CI support, or research and technology protection within a program office, laboratory, test and evaluation center, or other Research, Development, Test and Evaluation (RDT&E) organization should identify the proper contacts in these organizations prior to initiating program planning.

Functional Offices	Chapter 8 References
Security Support Office • Protection Planning for RDT&E Activities • Assignments, Visits, and Exchanges of Foreign Representatives • Collaboration • Foreign Collection Threat • Execution of the PPP	8.3.2.1 8.3.2.2 8.4.5.2 8.4.6.2 8.4.11

Counterintelligence Support Organization • CI Support at RDT&E facilities • Collaboration • CI analysis of CPI • CI input into the PPP • CI Support Plan	8.3.4 8.4.5.2 8.4.7 8.4.11 8.5.2
Designated Disclosure Authority per DoDD 5230.11 • Safeguarding DoD RDT&E Information • Programs with Foreign Participation • Collaboration • Technology Assessment/Control Plan • Providing Documentation to Contractors	8.3.1.2 8.4.3 8.4.5.2 8.4.8 8.4.9.6
Intelligence Support Organization • Intelligence	8.2
Intelligence Requirements Certification Office • Intelligence Certification	8.2.2
Government Industrial Security Office • Support from Cognizant Government Industrial Security Offices	8.4.9.7
Anti-Tamper Support Organization • Anti-Tamper • DoD Anti-Tamper Executive Agent	8.5.3
Operations Security • Collaboration	8.4.5.2

Defense Security Service • Counterintelligence Support During Pre-Acquisition	8.3.4

Table 8.0.5.T1. Functional Offices in Chapter 8

8.1. Introduction

8.1.1. General Information

The Department of Defense actively seeks to include allies and friendly foreign countries as partners in the Research, Development, Test and Evaluation (RDT&E); production; and support of defense systems. The Department of Defense encourages early involvement with allied and friendly foreign partners. Such cooperative foreign government partnerships should begin at the requirements definition phase, whenever possible. Successful execution of cooperative programs will promote the desirable objectives of standardization, commonality, and interoperability. The U.S. Government and its foreign government partners in these endeavors will benefit from shared development costs, reduced costs realized from economies of scale, and strengthened domestic industrial bases. Similarly, the Department of Defense plays a key role in the execution of security cooperation programs that ultimately support national security objectives and foreign policy goals. U.S. defense system sales are a major aspect of security cooperation.

Increasingly, the U.S. Government relies on sophisticated technology in its defense systems for effectiveness in combat. Further, technology is recognized as a force multiplier and will continue to improve the warfighter's survivability. Therefore, it is not only prudent, but also practical to protect technologies deemed so critical that their exploitation will diminish or neutralize a U.S. defense system's effectiveness. Protecting critical technologies preserves the U.S. Government's research and development resources as an investment in the future, rather than as an expense if technology is compromised and must be replaced prematurely. It also enhances U.S. industrial base competitiveness in the international marketplace.

When necessary and successfully applied, procedures and guidance in this chapter are designed to protect Critical Program Information (CPI) and Critical System Resources against compromise, from Research, Development, Test and Evaluation (RDT&E) throughout the acquisition life cycle (including property disposal), at all involved locations or facilities. CPI may be classified information or Controlled Unclassified Information about technologies, processes, applications, or end items that if disclosed or compromised, would degrade system combat effectiveness, compromise the program or system capabilities, shorten the expected

combat-effective life of the system, significantly alter program direction, or require additional RDT&E resources to counter the impact of the compromise. CPI includes, but is not limited to, CPI inherited from another program and CPI identified in pre-system acquisition activities or as a result of non-traditional acquisition techniques (e.g., Advanced Concept Technology Demonstration, flexible technology insertion). Air Force Policy Directive 63-17 defines Critical System Resources as, ". . .those resources that if unavailable or compromised, could seriously impact development, production, delivery, or operation of a system, component, or technology."

- The teamwork engendered by this chapter provides intelligence support to the analysis phase of capabilities integration and development prior to Milestone A. The teamwork also selectively and effectively applies research and technology protection countermeasures and CI support to the program, resulting in cost-effective activities, consistent with risk management principles, to protect CPI through the life cycle of the program.
- Anti-Tamper (AT) techniques and application of system security engineering measures allow the United States to meet foreign customer needs for advanced systems and capabilities while ensuring the protection of U.S. technological investment and equities. AT techniques and system security engineering measures are examples of protection methodologies that DoD programs use to protect critical system technologies.

8.1.2. Protection Overview

Critical Program Information (CPI) may include classified military information which is considered a national security asset that will be protected and shared with foreign governments only when there is a clearly defined benefit to the United States (see DoD Instruction 5200.39). It may also include Controlled Unclassified Information, which is official unclassified information that has been determined by designated officials to be exempt from public disclosure, and to which access or distribution limitations have been applied in accordance with national laws and regulations such as the International Traffic in Arms Regulations for U.S. Munitions List items and the Export Administration Regulations for commerce controlled dual-use items. In some cases (and this is dependent on the program manager's determination) a commercial-off-the shelf (COTS) technology can be designated CPI if the COTS element is determined to fulfill a critical function within the system and the risk of manipulation needs mitigation.

CPI requires protection to prevent unauthorized or inadvertent disclosure, destruction, transfer, alteration, reverse engineering, or loss (often referred to as "compromise").

CPI identified during research and development or Science and Technology should be safeguarded to sustain or advance the DoD technological lead in the warfighter's battle space or joint operational arena.

The CPI, if compromised, will significantly alter program direction; result in unauthorized or inadvertent disclosure of the program or system capabilities; shorten the combat effective life of

the system; or require additional research, development, test, and evaluation resources to counter the impact of its loss. See DoD Instruction 5200.39 for the definition of CPI.

The theft or misappropriation of U.S. proprietary information or trade secrets, especially to foreign governments and their agents, directly threatens the economic competitiveness of the U.S. economy. Increasingly, foreign governments, through a variety of means, actively target U.S. businesses, academic centers, and scientific developments to obtain critical technologies and thereby provide their own economies with an advantage. Industrial espionage, by both traditionally friendly nations and recognized adversaries, proliferated in the 1990s and has intensified with computer network attacks today.

Information that may be restricted and protected is identified, marked, and controlled in accordance with DoD Directives 5230.24 and 5230.25 or applicable national-level policy and is limited to the following:

- Information that is classified in accordance with Executive Order 12958, and
- Unclassified information that has restrictions placed on its distribution by:
- U.S. Statutes (e.g., Arms Export Control Act, Export Administration Act);
- Statute-driven national regulations (e.g., Export Administration Regulations (EAR), International Traffic in Arms Regulations (ITAR)); and
- Related national policy (e.g., Executive Order 12958, National Security Decision Directive 189).

Incidents of loss, compromise, or theft of proprietary information or trade secrets involving CPI, are immediately reported in accordance with Section 1831 et seq. of Title 18 of the United States Code, DoD Instruction 5240.04, and DoD Directive 5200.01. Such incidents are immediately reported to the Defense Security Service (DSS), the Federal Bureau of Investigation (FBI), or the applicable DoD Component CI and law enforcement organizations. If the theft of trade secrets or proprietary information might reasonably be expected to affect DoD contracting, DSS should notify the local office of the FBI.

DSS presently has responsibility for protecting CPI that is classified. However, the contract may specifically assign DSS responsibility to protect CPI that is controlled unclassified information. Consequently, DSS would receive reporting on unclassified CPI incidents if it had specific protection responsibility or the incident could involve foreign intelligence activity or violate the ITAR or EAR.

8.2. Intelligence

8.2.1. Threat Intelligence Support

8.2.1. Threat Intelligence Support

Intelligence support to the acquisition process provides an understanding of threat capabilities that is integral to the development of future U.S. military systems and platforms. Identifying projected adversarial threat capabilities, to include scientific and technical developments, which may affect a program or a capability's design or implementation is crucial to a successful development process. Furthermore, the applicable threat information must be continually updated to account for adversarial capabilities throughout the program or capability's projected acquisition to ensure technological superiority over adversarial capabilities is maintained. See the graphic in Figure 8.2.1.F1.

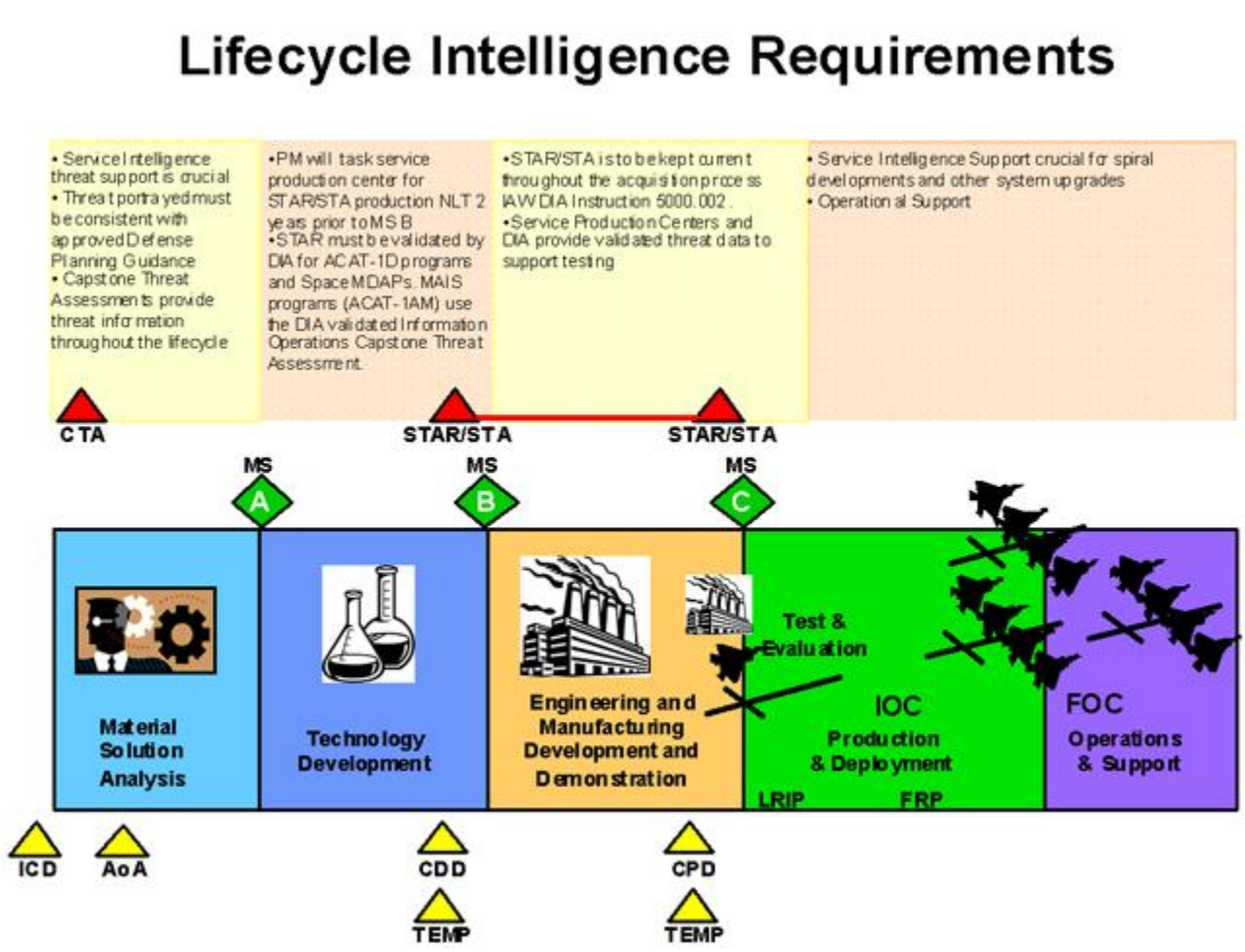


Figure 8.2.1.F1. Depiction of Life-Cycle Intelligence Requirements

Figure 8.2.1.T1 illustrates the range of support provided by the threat intelligence community over the life of a particular capability shortfall identification process and resulting system acquisition program. During the Joint Capabilities Integration and Development System (JCIDS) capability shortfall identification process, the capabilities community will obtain threat intelligence primarily from the Capstone Threat Assessments (CTAs). The CTAs project foreign capabilities in particular warfare areas looking out 20 years.

Once the JCIDS process identifies a materiel solution and the Material Solution Analysis phase begins, the program office should task the appropriate intelligence production center for the lead service to produce the System Threat Assessment Report (STAR) for Acquisition Category (ACAT) I/ Major Defense Acquisition Programs (MDAPs) and the System Threat Assessment (STA) for ACAT II programs in accordance with the regulations of that service. The program office needs to work with the producing intelligence center to provide system specific characteristics as they evolve. The program office must also work with the appropriate Service Intelligence Production Center to identify Critical Intelligence Parameters (CIPs) and ensure production requirements are levied against those CIPs.

As required by DoD Instruction 5000.02, STARs for ACAT ID MDAPs must be validated by the Defense Intelligence Agency (DIA). STARs for ACAT IC MDAPs and STAs for non-MDAPs will be validated by the lead service in accordance with service regulations. The producing center will convene a Threat Steering Group, co-chaired by DIA for ACAT ID MDAPs, to produce and review the STAR. The validated STAR/STA constitutes the primary threat reference for program development and testing. DoD Directive 5000.01 requires program managers to keep threat capabilities current and validated in program documentation throughout the acquisition process.

Major Automated Information System (MAIS) programs will use the DoD intelligence community-produced and DIA-validated Information Operations (IO) Capstone Threat Assessment. Non-MAIS programs are encouraged to use the IO Capstone Threat Assessment as their threat baseline. While the IO Capstone Threat Assessment provides the required threat documentation, MAIS programs still need to provide system descriptions, as well as the CIPs and production requirements that are specific to their program's needs.

Analytic Baseline. A system's Analytic Baseline is comprised of DoD-level authoritative policy planning guidance and an intelligence assessment of present trends and conditions, combined with validated parametric, characteristics/performance and employment data needed for development, testing, and/or training. When combined with information on appropriate friendly and neutral (Blue/Gray/White*) systems, it represents an extrapolation of the total security environment in which the system is expected to operate. A package comprises a scenario, concept of operations, and integrated data used by the DoD components as a foundation for strategic analyses. Examples of analytical baselines include scenarios and supporting data used for computer assisted war games and theater campaign simulations.

* The three colors reflect three different entities. Blue represents U.S. system data, Gray represents friendly system data, and White represents neutrals. When doing long term analysis, the impact of U.S./Blue systems must be taken in light of friendly, as well as neutral systems.

8.2.1.1. Capstone Threat Assessment (CTA)

CTAs address, by warfare area, current and future foreign developments that challenge U.S. warfighting capabilities (e.g., precision strike warfare, undersea warfare, space operations, surveillance, and reconnaissance). Most CTAs require input from multiple Defense Intelligence elements. With the lead intelligence production center, DIA's Defense Warning Office co-chairs the Threat Steering Group that produces and reviews the document. As CTAs support multiple programs, usually including ACAT- ID programs, they will be validated by DIA.

The DoD Intelligence Community (DoDIC) produces the Capstone Threat Assessments/Capstone System Threat Assessment Reports listed in Table 8.2.1.1.T1.

WARFARE AREA	PRIMARY PRODUCTION OFFICE / CENTER

Land Warfare	National Ground Intelligence Center (NGIC) *(U) Land Warfare Capstone Threat Assessment* Joint Worldwide Intelligence Communications System (JWICS): In production. Publication TBD Secret Internet Protocol Router Network (SIPRNET):
Air Warfare	National Air and Space Intelligence Center (NASIC) *(U) Air Warfare Capstone* JWICS http://www.naic.ic.gov/TableView/usthreat_pagetable.shtml SIPRNET http:storefront1s.naic.wrightpatterson.af.smil.mil/TableView/usthreat_pagetable.shtml
Chemical, Biological and Radiological Defense	Defense Intelligence Agency (DIA)/Counter Proliferation Support Office (CPT) *(U) Chemical, Biological, and Radiological Warfare Capstone Threat Assessment* JWICS: http://delphi.dia.ic.gov/admin/di/dwo3_files/Products/Assessments.htm SIPRNET: http://delphi.dia.smil.mil/admin/di/dwo3_files/Products/Assessments.htm
Information Operations	DIA/Joint Information Operations Threat Working Group *(U) Information Operations Capstone Threat Assessment* JWICS: http://delphi.dia.ic.gov/admin/di/dwo3_files/Products/Assessments.htm SIPRNET: http://delphi.dia.smil.mil/admin/di/dwo3_files/Products/Assessments.htm
Maritime	Office of Naval Intelligence (ONI) (currently published as Capstone System Threat

Warfare	Assessments on JWICS) *(U) Submarine Capstone STAR:* http://qdeck.nmic.ic.gov/PRODUCTS/new22/223/Sub_Capstone06/sc_cov.htm or http://seawolf.nmic.navy.smil.mil/PRODUCTS/new22/223/Sub_Capstone_06/SC_cov.htm *(U) Surface Ship Capstone STAR:* http://qdeck.nmic.ic.gov/PRODUCTS/ONI22/SAW/ONI-223_Acquisition_Sup/Sub_Programs/SS_CSTA%202006/ssccov.htm or http://seawolf.nmic.navy.smil.mil/PRODUCTS/new22/223/ss_CSTA_08/ss_For.htm *(U) Naval Fixed Wing Capstone STAR:* http://qdeck.nmic.ic.gov/PRODUCTS/new22/223/CSTA_FW/fw_cov.htm or http://seawolf.nmic.navy.smil.mil/PRODUCTS/new22/223/CSTA_2008/csta042108a/fw_for.htm
Missile Defense	DIA/Acquisition Support Division/Defense Warning Office (DWO-3) *(U) Missile Defense Threat Environments* JWICS: http://www.dia.ic.gov/admin/di/dwo/dwo3_files/Products/Assessments.htm SIPRNET: http://www.dia.smil.mil/admin/di/dwo/dwo3_files/Products/Assessments.htm
Space Warfare	NASIC *(U) Space Capstone Threat Assessment* JWICS:

	http://www.naic.ic.gov/TableView/usthreat_pagetable.shtml SIPRNET http://storefront1s.naic.wrightpatterson.af.smil.mil/TableView/usthreat_pagetable.shtml
Note: Web addresses provided in this table cannot be accessed from the unclassified Internet. The ".ic.gov" means this file is located on the Joint Worldwide Intelligence Communications System (JWICS) network which is a TS classified system. The ".smil.mil" means this file is located on the SIPRNET which is a Secret level classified system.	

Table 8.2.1.1.T1. Listing of Capstone Threat Assessments/Capstone System Threat Assessment Reports

8.2.1.2. System Threat Assessment Report (STAR)/System Threat Assessment (STA)

The Defense Intelligence Agency (DIA) provides validation for System Threat Assessment Reports (STARs), prepared by the appropriate Service, to support Acquisition Category (ACAT) ID/ Major Defense Acquisition Programs (MDAPs). Appropriate Defense Intelligence organization(s), identified by DIA, prepare the STAR. The assessment should be kept current and validated throughout the acquisition process. DoD Instruction 5000.02 requires that MDAPs have a validated STAR in place at Milestones B and C (and at program initiation for shipbuilding programs). The assessment should be system specific to the degree that the system definition is available at the time the assessment is being prepared. The assessment should address projected adversary capabilities at system initial operating capability (IOC) and at IOC plus 10 years. DIA Instruction 5000.002 describes STAR elements and format. STARs for ACAT IC MDAPs and STAs for ACAT II non-MDAPs are prepared and validated by the lead service in accordance with service regulations.

Program-provided Critical Intelligence Parameters (CIPs), and their associated production requirements, are a key part of a STAR and will be required for validation. The inclusion of CIPs is also encouraged for STAs.

CIPs are those key performance thresholds of foreign threat systems, which, if exceeded could compromise the mission effectiveness of the U.S. system in development. CIPs, and their accompanying production requirements, will be included in the STAR unless DIA's Acquisition Support Division in the Defense Warning Office (DWO-3), the Threat Steering Group, and the program office agree that CIPs are not required. If a CIP is breached, the responsible intelligence production center will notify the program office and DIA/DWO-3 in accordance with DIA Instruction 5000.002. DIA/DWO-3 will notify the appropriate organizations in the Office of the Secretary of Defense.

At the discretion of the lead service production center, Capstone STARs can be used to support multiple programs which share a common threat base. System description and CIPs will be provided for each program that the Capstone STAR covers.

8.2.1.3. Threat Validation

As noted above, for Major Defense Acquisition Programs (MDAPs) subject to Defense Acquisition Board review, the Defense Intelligence Agency (DIA) validates System Threat Assessment Reports (STARs) for Acquisition Category (ACAT) ID/ Major Defense Acquisition Programs (MDAPs). STARs for ACAT IC MDAPs and System Threat Assessments for ACAT II programs are validated by the appropriate service. DIA validation assesses the appropriateness and completeness of the intelligence, consistency with existing intelligence positions, and the use of accepted analytic tradecraft in developing the assessments. Working with its partners in the DoD intelligence community and, as needed, in the larger intelligence community, validation is intended to ensure that all relevant data is considered and appropriately used by author(s) of the assessment.

DIA validates threat information contained in Joint Capabilities Integration and Development System documents as described in the JCIDS Manual. When requested by appropriate authority, DIA may also validate other threat information not contained in the STAR but needed for program development.

8.2.1.4. Support to Operational Test and Evaluation

The Test and Evaluation Master Plan should define specific intelligence requirements to support program operational test and evaluation. When requested by the appropriate authority in the offices of the Director, Operational Test and Evaluation (DOT&E) or the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)), DIA, working with the Department of Defense Intelligence Community (DoDIC), will provide additional intelligence support to the operational testing of programs on the annual DOT&E Oversight List. DIA support will not include the validation of specific testing scenarios or the validation of "Blue" surrogate systems or platforms, but can include certification that the threat information in the test plan is correct and consistent with existing assessments.

Per DoD Instruction 5000.02 all programs on the DOT&E Oversight List are to be considered as MDAPs for testing and evaluation purposes and will require a Defense Intelligence Agency (DIA)- or DoD Component- validated System Threat Assessment Report regardless of Acquisition Category designation. DOT&E, Under Secretary of Defense (Intelligence), and DIA's Acquisition Support Division in the Defense Warning Office (DWO-3) will jointly determine which programs require a DIA validation, and which will require Service-level validation.

8.2.2. Intelligence Certification

The Joint Staff and Defense Intelligence Agency (DIA) provide review, coordination, and certification/endorsement functions in support of the Joint Capabilities Integration and Development System (JCIDS) process. These functions include intelligence certification and threat validation. All acquisition programs or capabilities that are expected to operate in a threat environment must be developed in accordance with the most current threat information. Per CJCS Instruction 3312.01, the applicable threat information must be continually updated to account for threats throughout the program or capability's projected acquisition life cycle. DIA's Acquisition Support Division in the Defense Warning Office (DWO-3) will assist sponsors with incorporating adversarial capabilities throughout the JCIDS review process, and will review and validate the threat input within the JCIDS documents.

Initial Capabilities Document (ICD). The initiating DoD Component prepares a concise threat summary and threat rationale, working with DIA/DWO-3 as needed. If validated Capstone Threat Assessments (CTAs) or System Threat Assessment Reports (STARs)/System Threat Assessments (STAs) are available and address the threat areas affecting the U.S. capability, these documents should be used as the primary sources for the threat statements. The ICD will reference the threat documents used to support the analysis.

Capability Development Document (CDD). The initiating DoD Component prepares a concise threat summary and threat rationale, working with DIA DWO-3 as needed. If validated CTAs or STARs/STAs are available and address the threat areas affecting the U.S. capability, these documents should be used as the primary sources for the threat statements. DoD components may use STAR or CTA formats as desired to organize the threat statement. Programs designated as ACAT-ID MDAPs, or programs with the potential to be so designated, must use DIA-validated threat references.

Capability Production Document (CPD). The initiating DoD Component prepares a concise threat summary and threat rationale, working with DIA/DWO-3 as needed. If validated CTAs or STARs/STAs are available and address the threat areas affecting the U.S. capability, these documents should be used as the primary sources for the threat statements. DoD Components may use STAR or CTA formats as desired to organize the threat statement. Programs designated as ACAT ID MDAPs, or programs with the potential to be so designated, must use DIA-validated threat references.

Additional Criteria. The certification also evaluates intelligence-related systems with respect to open system architecture, security, and intelligence interoperability standards. (J-6 Interoperability certification is conducted in a separate, but related process, and is documented in CJCS Instruction 6212.01.)

Those personnel with a SIPRNET terminal can access the specific procedures and criteria for the Intelligence Certification on the Intelligence Requirements Certification Office homepage (under "Certification Process"). By telephone, additional information may be obtained by calling the Intelligence Requirements Certification Office at 703-695-4693.

8.2.3. Signature Support

8.2.3. Signature Support

DoD Directive 5250.01, "Management of Signature Support within the Department of Defense," establishes the SSP (previously known as the National Signatures Program (NSP) to manage and execute the DoD Signature Support Mission (SSM). Signatures are essential for building target models, developing algorithms, optimizing sensor design, and validating sensor functionality. Program Managers (PM) should account for signatures during system and sensor acquisition. The PM documents detailed signature requirements in a LSSP (per DoD Directive 5250.01) and defines overall signature support requirements and compliance with signature standards in paragraph 9 of the Capability Development Document and Capability Production Document (per CJCS Instruction 3312.01, "Joint Military Intelligence Requirements Certification"). Under CJCS Instruction 3312.01, the SSP uses the Life-cycle Signature Support Plan to assess the ability of the signatures community to support a program's signature requirements.

8.2.3.1. Signature Support in the Acquisition Strategy

DoD Directive 5250.01 requires that signature support requirements and funding be incorporated into a program's Acquisition Strategy. If required signatures are not already available in the distributed national signatures pool, the program will need to plan and budget for development of these signatures. Stating in the Acquisition Strategy that a program is signature dependent and will identify requirements in a Life-cycle Signature Support Plan ensures that the Program Office has considered signature development needs in the program planning and budgeting process.

8.2.3.2. Distributed DoD Signatures Pool and Signature Standards

DoD Directive 5250.01 requires that all signatures produced for the DoD be made available through a distributed DoD signature pool and adhere to established signature standards. Whether developed by a government signature center or by a contractor, if the signatures are made available through a distributed pool, they can be shared and will help prevent duplication of work. An essential element to make this possible is the use of standards to ensure common meta-data tags and processing methods are used. This in turn ensures the signatures will be discoverable in the distributed pool, and that the signatures will be usable for multiple customers, including acquisition programs and operational systems. The Signatures Support Program provides single access point connectivity to the distributed pool through web-pages on JWICS (http://www.ssp.ic.gov/), SIPRNet (http://dt.dia.smil.mil/ssp), and NIPRNet (site under development). (NOTE: These sites cannot be accessed via the Internet or Non-secured Internet Protocol Router Network.) Current signature standards are also available at these web-sites.

8.2.3.3. Signature Support to the Materiel Solution Analysis Phase

The Signatures Support Program maintains signature enterprise information that may be useful during the Materiel Solution Analysis phase. This information includes:

- *Signature Dependent Sensors* – A master file of existing sensors is maintained and listed by signature discipline and sub-discipline, and also by organization in the DoD, Intelligence Community, and other government agencies. Awareness of existing sensors will be useful for the Analysis of Alternatives (AoA) and development of the Technology Development Strategy>.
- *Signature Technologies* – Signature Technology Research information and Emergent Technology Reports are available to foster technology transfer between agencies across the U.S. government. These reports may be useful for the AoA and TDS.
- *Acquisition Systems* – A listing of signature-dependent acquisition programs is available to foster cross program synergies and shared development. Programs are listed by signature discipline and sub-discipline, and also by organization in the DoD, Intelligence Community, and other government agencies. A one page system synopsis is available for each listed program. These summaries may be useful for the AoA and TDS.

8.2.3.4. Life-cycle Signature Support Plan (LSSP)

DoD Directive 5250.01 requires that an LSSP shall be established for signature dependent programs and shall be developed during the Material Solution Analysis and Technology Development phases. It also directs the Defense Intelligence Agency to establish the SSP to manage and execute the Signature Support Mission to accomplish the policy objectives of the directive.

To meet these requirements, the Program Manager needs to submit an LSSP to their Signatures Council representative prior to Milestone A, Milestone B, and Milestone C. The LSSPs should be submitted at the same time as the Initial Capabilities Document (Milestone A), Capability

Development Document (Milestone B), and Capability Production Document (Milestone C) deliveries respectively. The LSSP defines specific signature requirements for the acquisition phase of a program, and becomes more detailed as the system progresses toward Initial Operational Capability. For each required signature, as much detail as possible should be provided in the LSSP. LSSPs will facilitate the Intelligence Certification process relative to signatures.

Questions about the LSSP can be sent by e-mail (JWICS: DIDL465@dia.ic.gov, SIPRNet: SIDL001@dia.smil.mil, Unclass: NIDL135@dia.mil) or phoned-in by calling 1-877-238-8821.

The LSSP instructions and templates are available on the SSP web-pages:

- SIPRNet: http://dt.dia.smil.mil/ssp/
- JWICS: http://www.ssp.ic.gov/

8.2.3.4.1. Life-cycle Signature Support Plan (LSSP) prior to Milestone A

Since final material solutions have not yet been approved at this point, detailed signature requirements may not be known. However, based on the intended operational mission, the program should at least be able to identify the signature type (e.g., Radar, Thermal, Acoustic, etc.) and the threat domain (e.g., Space, Air, Land, Naval, Missile Defense, etc.) and possibly sub-categories within a threat domain (e.g., for Air: Fighter Aircraft) where signatures will be required. If specific target requirements are known, they should be stated. The initial LSSP may be included in the Technology Development Strategy(TDS).

8.2.3.4.2. Life-cycle Signature Support Plan (LSSP) prior to Milestone B

As a program approaches Milestone B, the LSSP needs to be updated with mission or capability specific details and threat signature requirements to support program development. For example, more details should be known about the mission of the sensor, technical parameters, and the threat target set. The program should also list any signature-based models that will be required, intelligence Production Requirements which have been submitted to a Service Intelligence Production Center (e.g., National Air and Space Intelligence Center, National Ground Intelligence Center, Office of Naval Intelligence, etc.), and planned signature collection events that the program will conduct.

8.2.3.4.3. Life-cycle Signature Support Plan (LSSP) prior to Milestone C

This LSSP will be an update to the previous LSSP. The purpose of this update is to add any new signature requirements due to target threat updates in preparation for operational status. This version of the LSSP must include a COCOM vetted list of prioritized targets required by Initial Operating Capability and Full Operating Capability for the program. It should define the signature production concept to be employed for the operational capability. As a minimum, these LSSPs should include information on signature developed within the program (modeling and simulation or measured physical parameters) for sensor or algorithm development or for testing purposes, and; information on the existence of any "blue" signatures collected for the program. Signature production specification should be cited and updated. Additionally, the signature production concept must be defined. At a minimum, this should include responsible entities for adversary signature production, commercial target signature production, and U.S. target (Blue) signature production. This information is required to ensure these signatures can be made available through the distributed DoD signature pool.

8.2.3.5. Life-cycle Signature Support Plan (LSSP) Assessment

Each LSSP will be assessed to identify existing signature holdings, requirements, standards, collection events and technologies relative to the program. As a result, a custom assessment is provided to the Program Manager (PM) to use in planning for signature collection, development, and processing to ensure signatures are available in time to meet system design and delivery schedules.

8.3. Pre-Acquisition Protection Strategy for Research, Development, Test and Evaluation (RDT&E) Activities

8.3.1. General

Protection may apply to all seven subcategories of RDT&E (see DoD 7000.14-R, Volume 2B). DoD Instruction 5200.39 recognizes the normally unrestricted nature of fundamental research, as identified in NSDD 189, and as further stipulated for Basic Research in Executive Order 12958. The term "fundamental research" refers generally to Basic Research (6.1) and Applied Research (6.2), and is defined in the ITAR (informative PowerPoint briefing).

8.3.1.1. Purpose

The purpose of pre-acquisition protection is to prevent unauthorized disclosure of DoD Research, Development, Test and Evaluation (RDT&E) information. Counterintelligence and security specialists provide a wide range of services to ensure personnel assigned to RDT&E sites are aware of threats from foreign intelligence services, other foreign interests, or anyone involved in unauthorized acquisition of DoD information. For example, one of these services can be to ensure requirements for authorized foreign involvement are met and that personnel administering such programs are well versed in those requirements.

8.3.1.2. Safeguarding DoD Research, Development, Test and Evaluation (RDT&E) Information

Working together, RDT&E laboratories and centers, and CI, security, foreign disclosure, operations security (OPSEC), and intelligence organizations should use an interactive process (such as an Integrated Product Team) to safeguard Critical Program Information (CPI) from compromise in order to sustain or advance the DoD technological lead in the future battle space.

- The RDT&E commanding officer, site director, or their designee (referred to hereafter as "site director") identifies their CPI, and communicates the results to CI, security, foreign disclosure, OPSEC, and intelligence organizations.
- The supporting CI organization, in consultation with the site director, prepares a site-specific CI Support Plan for each RDT&E site as well as academic and commercial facilities supporting the effort.
- Intelligence organizations provide information concerning technical capabilities that adversaries could use to gain information on specific RDT&E programs or projects.
- Site directors, in coordination with security, intelligence, and CI specialists, should ensure that assigned personnel receive tailored threat briefings.

8.3.2. Protection Approaches

RDT&E conducted within the DoD, as well as by DoD contractors, is covered by the following policies:

- Disclosure of both classified military information and unclassified technical data (DoD Directive 5230.11, "Disclosure of Classified Military Information (CMI) to Foreign Governments and International Organizations;" DoD Directive 5230.24, "Distribution Statements on Technical Documents;" DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure,"International Traffic in Arms Regulations (informative PowerPoint briefing), and Export Administration Regulations).
- Control of foreign visitors (DoD Directive 5230.20, "Visits, Assignments, and Exchanges of Foreign Nationals").
- Export control (DoD Directive 2040.02, "International Transfers of Technology, Goods, Services, and Munitions").

For effective protection, the site director (and gaining Program Manager) should integrate these policies into an overall protection strategy, to ensure the identification of Critical Program Information, the identification of the applicable safeguards, and the effective application of those safeguards. The Counterintelligence Support Plan aids the formulation of an effective protection program at each RDT&E site. Site directors make these policies effective within the RDT&E environment through training and awareness programs, particularly for unclassified internet and e-mail to prevent data spills and hacking.

8.3.2.1. Protection Planning for Research, Development, Test and Evaluation (RDT&E) Activities

To conduct effective Research and Technology Protection (RTP) planning, each RDT&E site director should:

- Review the site RDT&E program periodically and/or whenever there is a significant change in the program.
- Identify information within the RDT&E program that has already been marked for safeguarding (e.g., export control, distribution statement, special handling caveat).
- Apply the Critical Program Information (CPI) criteria to that information to determine if any of it meets the minimum criteria and if so designate that information as CPI.
- If CPI is identified, develop and write a Program Protection Plan (PPP)
- Ensure information identified as CPI is appropriately marked and disseminated (e.g., export control, distribution statement, special handling caveat).
- Select appropriate countermeasures to protect the CPI and identify counterintelligence (CI) support to be provided.
- Prepare a CI Support Plan (CISP), with supporting organizations (e.g., CI, information technology, security, foreign disclosure, OPSEC, intelligence), tailored to focus protection resources on the identified CPI. (The CISP identifies the CPI and serves as the "contract" between the individual RDT&E site director and the responsible CI support activity.)
- Communicate the CPI to CI, information technology, security, foreign disclosure, OPSEC, and intelligence organizations, as appropriate.

RDT&E site director should not:

- Release, provide, or discuss any intelligence data/assessments not authorized to foreign nationals.

8.3.2.2. Assignments, Visits, and Exchanges of Foreign Representatives

The site director should:

- Ensure that assignments, visits, and exchanges of foreign nationals are processed through appropriate channels.
- Ensure that a contact officer has been appointed for each foreign national and is informed of authorized disclosures.
- Establish a process prior to the visit, wherein the relevant technical Point of Contact and appropriate security and CI personnel communicate the purpose of the visit by the foreign national and the technology and/or program information to be discussed.
- Ensure the process for approving visits by foreign nationals includes dissemination of appropriate disclosure rules and restrictions to Research, Development, Test and Evaluation (RDT&E) personnel being visited.
- Ensure that foreign nationals are visually identifiable as required by DoD Directive 5230.20.
- Establish a process for archiving information about foreign national visits, including but not limited to, information about the visitor, reason for the visit, information disclosed, and any anomalous event that occurred during the visit.
- Ensure proposed Critical Program Information releases are reviewed and approved using provision(s) of an Information Exchange Program Agreement (formerly Data Exchange Agreement) prior to release.
- Ensure copies of all international agreements (including Memoranda of Understanding, Information Exchange Program Agreements, and Delegations of Disclosure Letters) relevant to their programs and related systems are maintained and readily accessible to all program personnel as well as supporting CI and security personnel.

RDT&E site director should not:

- Release, provide, or discuss any intelligence data/assessments not authorized to foreign nationals.

8.3.2.3. Export Control

The site director should:

- Establish a process whereby Research, Development, Test and Evaluation (RDT&E) personnel determine whether technical data or commodities at RDT&E facilities have been approved for export to foreign countries.
- Establish a focal point at each RDT&E site to determine whether a license for deemed exports is required when a foreign national visits the facility.

RDT&E site director shall not:

- Release, provide, or discuss any intelligence data/assessments not authorized to foreign nationals.

8.3.3. Information Assurance

All Information Technology network and systems storing, processing, or transmitting Critical Program Information shall be accredited in accordance with the DoD Information Assurance Certification and Accreditation Process (DIACAP) as described in DoD Instruction 8510.01. All other networks are encouraged to be DIACAP compliant.

8.3.4. Counterintelligence (CI) Support During Pre-Acquisition

The site director, in consultation with the supporting CI activity, should develop a CI Support Plan for each Research, Development, Test and Evaluation (RDT&E) site as described in section 8.5.2.

To support the RDT&E site directors, DoD Component CI agencies should:

- Assign CI specialists to support DoD RDT&E activities on or off military installations. The assigned CI specialist(s) will:
  - Provide full-time, tailored, protection support to major DoD RDT&E sites. ("On-call" support will be provided to other DoD RDT&E sites.)
  - Provide, in coordination with the DSS, CI support to DoD contractors and academic institutions working with DoD CPI.
- Ensure that appropriate security, research management, foreign disclosure, Operations Security, and acquisition program personnel are continuously appraised of foreign intelligence or other threat information relating to their RDT&E site and/or research project.
- Disseminate CI information and products to contractor facilities under Defense Security Service (DSS) cognizance and to other locations and officials that DSS may designate.
- Keep DSS informed of any threat to CPI that involve contractors under the cognizance of DSS. Providing classified threat information to contractors will be coordinated with DSS.
- Receive threat relevant information and analysis from DSS on the contractor sites under its cognizance

- Provide requested threat information to assist defense contractors in developing and updating their Technology Control Plans and protection of DoD CPI.

8.4. Acquisition Protection Strategy for Program Managers

8.4.1. Pre-Acquisition Considerations

Program protection planning, as described in section 8.3, should begin with the Joint Capabilities Integration and Development System (JCIDS). It is integral to the overall acquisition strategy, which is typically developed prior to formal designation of an acquisition program. The program manager identifies the resources needed (e.g., personnel, fiscal) to accomplish the evaluation and initiate protection as early as possible, but no later than entry into Milestone B.

8.4.2. Acquisition Program Protection - Initiation to Implementation

Critical Program Information (CPI) is the foundation upon which all protection planning for the program is based, and the reason all countermeasures are implemented. Effective program protection planning begins by the program manager reviewing the acquisition program to determine if it contains CPI. If a program manager (PM) has not been appointed, the responsible commander/manager or program executive conducts this review. This examination should

consider CPI previously identified by DoD laboratories, CPI inherited from another program, or CPI that results from non-traditional acquisition techniques.

- The PM (or other official as noted above), with the assistance of a Working-Level Integrated Product Team (WIPT), determines the existence of CPI.
- If a program contains CPI, program protection planning is required (see 8.4.5). The PM (or other official as noted above), with the assistance of a WIPT and/or appropriate support activities, is responsible for developing and implementing a Program Protection Plan (PPP) (see 8.4.6).
- The PPP will be developed, as required, beginning in the Technology Development phase, and will be available to the Milestone Decision Authority at Milestone B and all subsequent milestones during the life cycle of the program. The PPP is revised and updated once every three years, or as required by changes to acquisition program status or the projected threat.
- If there is no CPI associated with the program (either integral to the program or inherited from a supporting program), the PM so informs the Milestone Decision Authority, Program Executive Officer, or DoD Component Acquisition Executive, as appropriate, and a PPP is not required.
- The next step is for the PM, through the program management staff, to translate protection requirements into a PPP. This is usually accomplished by a WIPT following the process outlined in section 8.4.6. Program protection activities described in sections 8.5.1 to 8.5.6.2 are tailored and performed prior to each milestone to provide the required countermeasures during each acquisition phase.
- After the protection planning foundation is laid, the program proceeds through the milestones and phases of the acquisition process. The program follows an event-based schedule that implements the protection strategy and completes the actions outlined in the PPP.

8.4.3. Programs with Foreign Participation

For a cooperative program, a Technology Assessment/Control Plan (TA/CP) should be done in each and every event. It is the key document that leads the analysis to identify CPI and other sensitive information (as contained in the definition of TA/CP IAW DoD Instruction 5200.39) that needs to be protected.

The Technology Control Plan (TCP), required under DoD 5220.22-M at cleared locations with foreign national visitors or employees, including those under Foreign Operated, Control, or Influence, and the TA/CP are similar but do not substitute for one another. The sites facility security officer should assure capability of the TCP and the TA/CP and the technologies addressed.

When a determination is made that any of the following conditions exist, a Technology Assessment/Control Plan (TA/CP) and a Delegation of Disclosure Authority Letter (DDL) should be prepared as annexes to the Program Protection Plan (PPP):

- Foreign participation in system development is possible;
- An allied system will be used;
- The system to be developed is a candidate for foreign sales or direct commercial sales;
- The system will be used in multinational operations; or
- The program will involve cooperative research and development (R&D) with allied or friendly foreign countries.

Under any of the above conditions, the Designated Disclosure Authority should be involved and informed. With respect to cooperative R&D programs, a Summary Statement of Intent, which includes a summarization of the TA/CP, is needed prior to obtaining authority to negotiate the International Agreement that is statutorily required to conduct the program.

If foreign involvement is initiated prior to the appointment of a program manager (PM), the DoD Component generating the capability need should prepare the TA/CP and DDL for Joint Requirements Oversight Council validation and Milestone Decision Authority approval. The PM, when appointed, should review the requirements for the PPP, TA/CP, DDL, and supporting documentation, and direct the preparation as appropriate.

8.4.4. Risk Management

8.4.4. Risk Management

The overall risk management effort should seamlessly span Systems Engineering and Program Protection, thus allowing a common vernacular for both. Risk management considerations should be a part of both the acquisition strategy and technology protection.

8.4.4.1. Risk Management in Systems Engineering

In systems engineering, risk management examines all aspects of the program as they relate to each other, from conception to disposal. This risk management approach integrates design (performance) requirements with other life-cycle issues such as manufacturing, operations, and support.

The program manager should establish a risk management process within systems engineering that includes risk planning, risk assessment (identification and analysis), risk management, and risk monitoring approaches to be integrated and continuously applied throughout the program, including the design process.

This type of risk assessment includes identification and analysis of potential sources of risk, to include cost, schedule, and performance, and is based on such factors as: the technology being used and its relationship to design; manufacturing capabilities; potential industry sources; and test and support processes.

8.4.4.2. Risk Management in Program Protection

In program protection, when viewed within the global context of security, risk management is concerned with technology transfer and is a systematic methodology to identify, evaluate, rank, and control inadvertent loss of technology. In this respect, it is based on a three-dimensional model: the probability of loss, the severity if lost, and the countermeasure cost to mitigate the loss. As such, risk management is a key element of a program manager's executive decision-making - maintaining awareness of technology alternatives and their potential sensitivity while making trade-off assessments to translate desired capabilities into actionable engineering specifications.

To successfully manage the risk of technology transfer, the program manager should:

- Identify contract vehicles which involve the transfer of sensitive data and technology to partner suppliers;
- Evaluate the risks that unfavorable export of certain technologies could pose for the program; and
- Develop alternatives to mitigate those risks.

8.4.5. Program Protection Planning

8.4.5. Program Protection Planning

When the acquisition program contains Critical Program Information (CPI), the program manager (PM) should initiate a program protection planning process that includes the following steps:

- Identify and set priorities on those operational or design characteristics of the system that result in the system providing unique mission capabilities.
- Identify CPI related to distinctive system characteristics in terms of their importance to the program or to the system being developed. (CPI includes defense technologies and their support systems as defined in DoD Instruction 5200.39.)
- Identify specific program locations where CPI is developed, produced, analyzed, tested, maintained, transported, stored, or used in training.
- Identify the foreign collection threat to the program. (Counterintelligence Analysis for CPI are discussed in section 8.4.7)
- Identify program vulnerabilities to specific threats at specific times and locations during all phases of the acquisition cycle.
- Identify time- or event-phased Research and Technology Protection (RTP) countermeasures to be employed by the program manager to reduce, control, or eliminate specific vulnerabilities to the program to ensure a minimum level of protection for CPI.
- Identify AT techniques (see section 8.5.3) and system security engineering (SSE) measures (see section 8.5.1) required to protect CPI. Ensure these AT and SSE techniques are included the system's design specifications, subsequent technical drawings, test plans, and other appropriate program documentation.
- Identify elements that require classification and determine the phases at which such classification should occur and the duration of such controls. The resulting program Security Classification Guide is issued by the program Original Classification Authority.
- Identify protection costs associated with personnel, products, services, equipment, contracts, facilities, or other areas that are part of program protection planning, and countermeasures. These costs are reflected in the program Planning, Programming, Budgeting and Execution process documentation.
- Identify the risks and benefits of developing, producing, or selling the system to a foreign interest, as well as the methods used to protect CPI if such an arrangement is authorized. Determine if an export variant is necessary (see section 8.5.1.5).
- Identify contractual actions required to ensure that planned SSE, AT techniques, information assurance, information superiority, classification management and/or RTP countermeasures are appropriately applied by defense contractors at contractor locations (see section 8.5.6). Care should be taken to ensure that measures do not adversely impact the technology of future foreign partners.
- Coordinate with program managers of supporting programs to ensure that measures taken to protect CPI are maintained at an equivalent level throughout DoD and its supporting contractors.

After completing the protection planning process, the program manager, assisted by applicable CI and security support activities, ensures implementation of countermeasures to protect the CPI at each location and activity identified in the protection planning process. The protection planning process is a dynamic and continuous element, and should remain amenable to appropriate revision.

8.4.5.1. Critical Program Information (CPI)

CPI is defined as elements or components of an Research, Development and Acquisition program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability. Includes information about applications, capabilities, processes, and end-items; Includes elements or components critical to a military system or network mission effectiveness; Includes technology that would reduce the US technological advantage if it came under foreign control. (DoD Instruction 5200.39).

CPI may include components; engineering, design, or manufacturing processes; technologies; system capabilities and vulnerabilities; and other information that give the system its distinctive operational capability. (Example: A system characteristic might be the small radar cross section. The CPI are those unique program elements that make the small radar cross-section possible.)

When CPI are inherited from a technology project and incorporated into an acquisition program, the Program Manager should incorporate the countermeasures prescribed in the PPP of origin until such time the CPI can be assed to determine whether it still requires protection during acquisition, or if new or related CPI exists.

8.4.5.1.1. Identifying Critical Program Information (CPI)

To develop the list of CPI, a Working-Level Integrated Product Team should refer to a functional decomposition already performed by the program office, or if necessary, perform a "functional decomposition" of the program or system, as follows:

- Analyze the program or system description and those specific components or attributes that give the system its unique operational capability.
- Analyze each subcomponent until a specific element is associated with each system capability.
- When a specific element is isolated, evaluate its potential as CPI by applying the following questions; an affirmative answer will qualify the item as CPI. If a foreign interest obtained this item or information:
    - Could a method be developed to degrade U.S. system combat effectiveness?
    - Could it compromise the U.S. program or system capabilities?
    - Would it shorten the expected combat-effective life of the system or significantly alter program direction?
    - Would additional Research, Development, Test and Evaluation resources be required to develop a new generation of the U.S. system that was compromised?
    - Would it compromise the U.S. economic or technological advantage?
    - Would it threaten U.S. National Security?
- In addition to the elements organic to the system, the program manager should consider any engineering process, fabrication technique, diagnostic equipment, simulator, or other support equipment associated with the system for its identification as a possible CPI. Special emphasis should be placed on any process that is unique to the system being

developed. The program manager and program engineer should evaluate each area and identify any activity distinctive to the U.S. industrial and technological base that limits the ability of a foreign interest to reproduce or counter the system.

8.4.5.1.2. Refining Critical Program Information (CPI)

Once all system CPI has been identified, additional refinement may be necessary. Key considerations in this refinement follow:

- Describe CPI in terms understandable by those not in the scientific or engineering field (e.g., use terms from the Militarily Critical Technology List or National Disclosure Policy). The fact that a particular technology is on a technology control list does not mean that particular technology is a CPI.
- Provide specific criteria for determining whether CPI has been compromised.
- Indicate any CPI related to a treaty-limited item.
- Indicate if this CPI is being or may be used by any other acquisition program or system.
- Prioritize CPI to ensure that the most important information is emphasized during protection cost analysis. That process addresses the following three questions:
    - What is the threat to U.S. National Security?
    - What is the extent to which the CPI could benefit a foreign interest?
    - How difficult is it for a foreign interest to exploit the information?

8.4.5.1.3. Inherited Critical Program Information (CPI)

The program manager (PM) should identify CPI for any component, subsystem, technology demonstrator, or other independent research program that will be incorporated into the PM's program. The using PM should ensure such CPI is addressed in the subsystem Program Protection Plan (PPP). Conversely, the PM of a subsystem program with CPI should ensure that their CPI is included in the major program PPP.

- The PM of a new system will ensure that CPI shared or gained from a subsystem is protected in the new system to at least the same level of protection afforded in the subsystem program.
- A PM of a system that incorporates a subsystem not reviewed to identify CPI should request the subsystem program office to review their program and supply the resulting information and/or documentation.
- When supporting activities defined as acquisition programs have not developed a PPP to protect their CPI, the PM incorporating the technology in question should request the subsystem PM to develop and provide an approved PPP.

8.4.5.2. Collaboration

The program manager (PM) is responsible for developing, approving, and implementing a Program Protection Plan (PPP), normally through a Working-level Integrated Product Team (WIPT). The PM may establish a research and technology protection WIPT or include the appropriate personnel on an existing WIPT to assist in preparing the PPP and its supporting documentation.

Counterintelligence (CI) and security support activities and program protection staff elements should assist the PM in identifying Critical Program Information.

The following personnel or organizational representatives are normally represented in the Research and Technology Protection (RTP) WIPT:

- Program office engineering and/or technical staff
- System user representative
- Maintenance and logistics representative
- Organizational or command security manager
- CI
- Intelligence
- Operations Security
- Foreign disclosure
- Base, installation, or post physical security staff
- Organization RTP staff representative
- Information Assurance Manager and/or information systems security manager

The PM should ensure close coordination and cooperation between the security, foreign disclosure, intelligence, operations security, CI, physical security, and RTP offices and the program office staff during development of a PPP.

8.4.6. Program Protection Plan (PPP)

8.4.6. Program Protection Plan (PPP)

The PPP is the program manager‘s (PM's) single source document used to coordinate and integrate all protection efforts designed to deny access to Critical Program Information (CPI) to anyone not authorized or not having a need-to-know and prevent inadvertent disclosure of leading edge technology to foreign interests. If there is to be foreign involvement in any aspect of the program, or foreign access to the system or its related information, the PPP will contain provisions to deny inadvertent or unauthorized access.

The PM establishes and approves the PPP for an acquisition program as soon as practicable after validation of the Initial Capabilities Document and the determination that CPI exists.

Preparation and implementation of a PPP is based on effective application of a systematic risk management methodology, not risk avoidance. Costs associated with protecting CPI are balanced between protection costs and potential impact if compromised. In some cases, residual risks may have to be assumed by the program; such decisions rest with the Milestone Decision Authority, based upon the recommendation of the PM.

The following guidance describes the process used to prepare a PPP when one is required:

- Any program, product, technology demonstrator, or other item developed as part of a separate acquisition process, and used as a component, subsystem, or modification of another program, should publish a PPP.
- Effectiveness of the PPP is highly dependent upon the quality and currency of information available to the program office.
    - Coordination between the program office and supporting CI and security activities is critical to ensure that any changes in the system CPI, threat, or environmental conditions are communicated to the proper organizations.
    - Intelligence and CI organizations supporting the program protection effort should provide timely notification to the PM of any information on adverse foreign interests targeting their CPI without waiting for a periodic production request.

The PPP is classified according to content.

The degree of detail in the PPP should be limited to information essential to plan and program the protection of CPI, and to provide an executable plan for implementing the associated countermeasures throughout the pre-acquisition and acquisition phases. While there is no specific format for PPPs, they normally include the following:

- System and program description;
- All program and support points of contact;
- A list of program CPI;
- Counterintelligence (CI) Analysis of CPI;
- Vulnerabilities of CPI;

- All Research and Technology Protection (RTP) countermeasures (e.g., anti-tamper techniques, system security engineering) and Militarily Critical Technology List citations for applicable CPI;
- All RTP associated costs, by Fiscal Year, to include PPP development and execution;
- CI Support Plan;
- Current Security Classification Guide;
- Foreign disclosure, direct commercial sales, co-production, import, export license or other export authorization requirements, and/or Technology Assessment/Control Plan; and
- Delegation of Disclosure Authority Letter, if appropriate.
- Program Security Instruction, if appropriate.

The following sections provide specific guidance related to some PPP topics listed above.

8.4.6.1. System and Program Descriptions

System Description. Since most acquisition programs combine existing, proven technology, as well as information with state-of-the-art technology, the system description included in a Program Protection Plan provides the reviewer with a clear indication of the capabilities and limitations of the system being acquired, including simulators and other supporting equipment. The purpose of the system description is to set the stage for identifying CPI. The system description should be based on the approved Initial Capabilities Document and Capability Development Document and include:

- Anticipated employment of the system within the battle space, along with the strategic, operational, or tactical impact of the system; and
- Specific characteristics that distinguish the system from existing systems, other systems under development, or that provide the system with unique operational or performance capability.

Program Description. This section is a short summary of the organization and structure of the office responsible for developing and fielding the acquisition system. Early in the acquisition process, that information may be somewhat limited. Detail should be added as participants in the program are identified and as their role in program protection activities becomes known. The program description should briefly describe the following:

- The program management chain of command, including the Program Executive Officer, DoD Component Acquisition Executive, and/or Milestone Decision Authority for the program and supporting programs;
- The locations, points of contact, and telephone numbers of prime contractors, sub-contractors, vendors, DoD sites, Federal agencies, Government Owned - Contractor Operated and DoD Research, Development, Test and Evaluation activities and/or facilities that will handle, store, or analyze CPI-related material;
- DoD Component and/or other DoD organization partners that are equity holders; and

- Likelihood that these technologies or this program will transition to another DoD Component / DoD organization in the future.

8.4.6.2. Foreign Collection Threat

Foreign collection threat assessment used by the program office in planning protection for the Critical Program Information (CPI) should be based upon a National-level intelligence estimate known as a "Counterintelligence (CI) Analysis of CPI."

- The CI Analysis of CPI is prepared and produced as a stand-alone document by the applicable DoD CI analysis center (see section 8.4.7);
- The CI Analysis of CPI should not be confused with a System Threat Assessment; the CI Analytical Product identifies foreign interests having a collection requirement and a capability to gather information on the U.S. system being developed;
- Sudden changes in the operational threat should be reviewed as they occur to determine if the changes are due to successful foreign intelligence collection;
- The program manager (PM) and Working-level Integrated Product Team should compare results of the CI Analytical product with the CPI and vulnerabilities to determine the level of risk to the program; and
- The WIPT should integrate environmental factors and arms control-related issues that might reduce the ability of foreign interests to collect information at a given location in the CI Analytical product, where applicable.

A threat exists when:

- A foreign interest has a confirmed or assessed requirement for acquiring specific classified or sensitive defense information or proprietary or intellectual property information;
- A foreign interest has the capability to acquire such information; and/or
- The acquisition of such information by the foreign interest would be detrimental to U.S. interests.

Confirmed or assessed identification of foreign collection requirements provide indicators of probable sources or methods employed to satisfy a collection requirement.

CI and security support activities assist the program office in preparing collection requirements and production requests to applicable DoD Component intelligence or CI analysis centers.

- CI and security support activities should submit the request to the intelligence center that normally supports the PM; and
- An informational copy is sent to the intelligence analysis center of any other DoD Component involved in the program to facilitate a single and unified position on the collection threat.

8.4.6.3. Vulnerabilities

Vulnerability is the susceptibility to compromise of a program to a threat in a given environment. Vulnerabilities to the program's Critical Program Information (CPI) are based upon one or more of the following:

- How CPI is stored, maintained, or transmitted (e.g., electronic media, blueprints, training materials, facsimile, modem);
- How CPI is used during the acquisition program (e.g., bench testing, field testing);
- Emanations, exploitable signals, or signatures (electronic or acoustic) that are generated or revealed by the CPI (e.g., telemetry, acoustic energy, radiant energy);
- Where CPI is located (e.g., program office, test site, contractor, academia, vendor);
- Types of Operations Security indicators or observables that are generated by program or system functions, actions, and operations involving CPI;
- Conferences, symposia, or foreign travel that the program manager (PM) and staff members participate in or plan to be involved in;
- The level of human intelligence or insider threat that is evident or projected at the program management location or other locations where CPI will be located;
- Foreign disclosures that are planned, proposed, or staffed for release;
- Degree of foreign participation that is currently pursued or being planned for the program or locations where CPI will be located.

The PM should prioritize identified vulnerabilities:

- Prioritization is based upon the consequences if CPI is lost or compromised, and the level of difficulty for a foreign interest to exploit the information; and
- Factors to be considered include the adverse impact on the combat effectiveness of the system, the effect on the combat-effective lifetime, and the cost associated with any modifications required to compensate for the loss.

8.4.6.4. Research and Technology Protection (RTP) Countermeasures

These are measures employed to eliminate or reduce the vulnerability of Critical Program Information (CPI) to loss or compromise, and include any method (e.g., anti-tamper techniques, information assurance) that effectively negates a foreign interest capability to exploit CPI vulnerability.

RTP countermeasures are developed to eliminate vulnerabilities associated with an identified threat to CPI based upon the authoritative, current, and projected threat information in the Counterintelligence Analysis of CPI. RTP countermeasures will:

- Be applied in a time- or event-phased manner (e.g., for certain periods of time, until milestones within program development).
- Be implemented until they are no longer required. They are terminated or reduced as soon as practicable after the threat, CPI, or environmental changes lead to a reduction or elimination of the vulnerabilities or a negation of the threat. For example, arms control countermeasures might be implemented only while the facility is vulnerable to a mandated arms control treaty inspection or an over flight by foreign inspectors.
- Address DoD Information Assurance and Certification and Accreditation Process compliance for all information technology systems and/or networks

The program manager (PM) should establish a countermeasures program based upon threat, risk management, Operations Security methodology, and vulnerability assessments. The PM should determine the costs associated with countermeasure application or implementation, and compare them to the risk associated with loss or compromise of the CPI. Whenever countermeasures to reduce, control, or eliminate a CPI vulnerability will not be developed, the PM should provide a justification for that decision in the countermeasures section of the Program Protection Plan (PPP).

If the acquisition program does not have an assigned or contracted security organization, applicable counterintelligence and security support activities should assist the program office in developing a draft countermeasures concept based upon the PM's guidance. The PM should designate the element of the program office responsible for publishing the PPP.

Additional RTP countermeasure considerations include the following:

- Countermeasures recommended to eliminate or reduce vulnerabilities associated with CPI at government and contractor facilities, may not be waived while the affected facilities are vulnerable to arms control treaty inspections or over flights by foreign interests.
- The requirement for contractor compliance with the government-approved PPP is included in the government solicitation and the resulting contract(s) (see section 8.4.9).
- Training in protection of research and technology information and security awareness is integral to the countermeasures effort.
    - Following approval of the PPP, the PM should implement a training program to inform all program members of the requirements in the PPP and, if applicable, the requirements and guidelines established in the Delegation of Disclosure Authority Letter, which is a U.S.-only document.
    - Emphasis is placed on encrypting the transmission of electronic messages, facsimile transmissions, and telephone transmissions relating to CPI, underpinning technologies, and other Controlled Unclassified Information related to programs containing CPI. These transmissions should be via Federal Information Processing Standard 140-2 compliant encryption.
- Countermeasures are dynamic. As the threat, CPI, or environment changes, the countermeasures may also change. The PM should update the PPP as system

vulnerabilities change, and thus reduce the cost of and the administrative burden on their program.

8.4.6.5. Security Classification Guide (SCG)

When necessary, the Program Manager must develop a SCG in accordance with DoD 5200.1-R and DoD 5200.1-H. The SCG addresses each Critical Program Information, as well as other relevant information requiring protection, including export-controlled information and sensitive but unclassified information.

All controlled unclassified information, information identified as For Official Use Only (FOUO) as defined in DoD 5400.7-R, or information with other approved markings that require dissemination controls (e.g., DoD Directive 5230.24 and DoD Directive 5230.25, is exempt from mandatory disclosure under the Freedom of Information Act and will be identified in the SCG.

The SCG will be reviewed, and amended when necessary, as part of each milestone review or as otherwise required by DoD 5200.1-R.

All intelligence related data/assessments will be classified in accordance with appropriate classification guidance and is not under the program manager's authorization.

8.4.6.6. Operations Security (OPSEC) Plan

When necessary, the program manager must develop an Operations Security (OPSEC) Plan in accordance with DoDD 5205.02 and DoDD 5205.02-M. The OPSEC Plan addresses each Critical Program Information, as well as other relevant program information requiring protection.

8.4.6.7. Protection Costs

Cost data associated with countermeasures and other Research and Technology Protection (RTP) efforts are compiled by the RTP Working-level Integrated Product Team, tabulated by acquisition phase, and included in the Program Protection Plan (PPP). Cost accounting only addresses the costs specific to the implementation of the PPP and excludes projected costs for operating with classified information. (See section 8.4.9.5)

Costs should be displayed by security discipline (e.g., physical security, personnel security, industrial security) and category (e.g., equipment, services, personnel). Cost data for each phase should be as specific as possible. Additionally, actual annual costs for the previous phase should be compiled and compared with the projected annual cost for the current acquisition phase. Significant deltas showing differences between projected and actual cost data should be explained. This information is used for justifications required by the Planning, Programming, Budgeting and Execution process.

The Acquisition Program Baseline includes costs related to PPP implementation.

8.4.7. Counterintelligence (CI) Analysis of Critical Program Information (CPI)

8.4.7. Counterintelligence (CI) Analysis of Critical Program Information (CPI)

When an acquisition program containing CPI is initiated, the Program Manager (PM) should request a CI Analysis of CPI from the servicing CI organization. The CI Analysis focuses on how the opposition sees the program and on how to counter the opposition's collection efforts. The CI analyst, in addition to having an in-depth understanding and expertise on foreign intelligence collection capabilities, must have a good working knowledge of the U.S. program. Therefore, CI organizations need information that describes the CPI and its projected use to determine the foreign collection threat to an acquisition program.

The CI Analytical product that results from the analysis will provide the PM with an evaluation of foreign collection threats to specific program or project technologies, the impact if that technology is compromised, and the identification of related foreign technologies that could impact program or project success. The CI analytical product is updated as necessary (usually prior to each major milestone decision) throughout the acquisition process. Changes are briefed to the program or project manager within 60 days.

When gathering information to meet the needs described in this Chapter, intelligence and CI organizations must comply with DoD Directive 5240.01 and DoD 5240.1-R. Information gathered by non-intelligence community entities must comply with DoD Directive 5200.27.

8.4.7.1. Requesting Counterintelligence (CI) Analytical Support

The Program Manager (PM)'s request to the counterintelligence organization for an analytical product normally contains the following information and is classified according to content:

- Program office, designator, and address;
- PM's name and telephone number;
- Point of contact's (POC's) name, address, and telephone number;
- Supporting or supported programs' or projects' names and locations;
- Operational employment role, if any;
- List of CPI;

- Relationship to key technologies or other controlled technology lists of the Departments of Defense, Commerce, and/or State;
- CPI technical description, including distinguishing characteristics (e.g., emissions; sight or sensor sensitivities) and methods of CPI transmittal, usage, storage, and testing;
- Use of foreign equipment or technology during testing (if known);
- Anticipated foreign involvement in the development, testing, or production of the U.S. system;
- Contractor names, locations, POCs, and telephone numbers, as well as the identification of each CPI used at each location; and
- Reports of known or suspected compromise of CPI.

8.4.7.2. Preliminary Counterintelligence (CI) Analytical Product

After the request is submitted, the DoD Component CI organization provides a preliminary CI Analytical product to the program manager within 90 days. A preliminary analytical product is more generic and less detailed than the final product. It is limited in use since it only provides an indication of which countries have the capability to collect intelligence on the U.S. system or technology as well as the possible interest and/or intention to collect it. The preliminary CI Analytical product may serve as the basis for the draft Program Protection Plan.

8.4.7.3. Final Counterintelligence (CI) Analytical Product

The program manager approves the Program Protection Plan only after the final CI Analysis of Critical Program Information (CPI) has been received from the applicable DoD Component CI and/or intelligence support activity. Normally, the CI Analysis of CPI is returned to the requesting program office within 180 days of the CI and/or intelligence organization receiving the request.

The CI Analysis of CPI answers the following questions about CPI:

- Which foreign interests might be targeting the CPI and why?
- What capabilities does each foreign interest have to collect information on the CPI at each location identified by the program office?
- Does evidence exist to indicate that a program CPI has been targeted?
- Has any CPI been compromised?

8.4.8. Technology Assessment / Control Plan (TA/CP)

8.4.8.1. General

The policy on Technology Assessment/Control Plan (TA/CP) is in DoD Directive 5530.3.

Prior to formal negotiation, the program manager prepares a TA/CP, or similar document, as part of the Program Protection Plan (PPP) for all acquisition programs with international involvement. The TA/CP is included in the PPP when it is determined that there is likely to be foreign involvement in the development program or when there will be foreign access to the resulting system or related Critical Program Information, by virtue of foreign sales, co-production, follow-on support, exchange program, training, or multinational exercises or operations. Much of the information required for the preparation of the TA/CP can be obtained from the Initial Capabilities Document / Capability Development Document, the Analysis of Alternatives (AoA), the Acquisition Strategy, and the justification and supporting information used in preparing those documents.

8.4.8.2. Purpose

The Program Manger (PM) uses the Technology Assessment/Control Plan (TA/CP) to do the following:

- Assess the feasibility of U.S. participation in joint programs from a foreign disclosure and technical security perspective.
- Prepare guidance for negotiating the transfer of classified information and critical technologies involved in international agreements.
- Identify security arrangements for international programs.
- Provide a basis for the Delegation of Disclosure Authority Letter that contains specific guidance on proposed disclosures.
- Support the acquisition decision review process.
- Support decisions on foreign sales, co-production, or licensed production, commercial sales of the system, or international cooperative agreements involving U.S. technology or processes.
- Support decisions on the extent and timing of foreign involvement in the program, foreign sales, and access to program information by foreign interests.

When it is likely there will be foreign involvement in the program, or foreign access to the resulting system or related information, it is advantageous for the program manager to prepare the TA/CP after completing the identification of CPI and Security Classification Guide (SCG). The TA/CP analysis often assists in developing vulnerabilities and proposed RTP countermeasures. Policies governing the foreign disclosure of intelligence information are in Intelligence Community Directive (ICD) 301 and Director of Central Intelligence Directive (DCID) 6/7*, and nuclear information governed by the Atomic Energy Act. These documents must be consulted when these types of information are involved in an acquisition program. *

This document may be found at Director of National Intelligence SIPRNET website: http://capco.dssc.sgov/frames/dcid/new/DCID%206-7/DCID%206-7.htm.

8.4.8.3. Content

The Technology Assessment/Control Plan (TA/CP) is composed of four sections: the "Program Concept"; the "Nature and Scope of the Effort and the Objectives"; the "Technology Assessment"; and the "Control Plan." Those TA/CP subsections are the basis for preparing the Delegation of Disclosure Authority Letter.

Program Concept. This section requires a concise description of the purpose of the acquisition program. It should describe, in the fewest words possible, the purpose of the system and the system threat or the military or technical requirements that created the need for the system. The description must be consistent with the Program Protection Plan.

Nature and Scope of Effort and the Objectives. This section briefly explains the operational and technical objectives of the program (e.g., co-production, cooperative research and development) and discusses any foreign participation or involvement. If foreign participation or involvement or the release of information to support potential foreign sales is considered likely, the phasing and disclosures at each phase should be described briefly. The milestones, foreign entities expressing interest, and summary of expected benefits to the U.S. should also be covered. The point of contact for all aspects of the TA/CP must be identified, including address, telephone numbers, and facsimile numbers.

Technology Assessment. The third section is the most important part of the TA/CP. It analyzes the technology involved in the program, its value, and the consequences of its compromise. It should provide conclusions regarding the need for protective security measures and the advantages and disadvantages of any foreign participation in the program, in whole or in part, and should describe foreign sales. The assessment should be specific concerning the phased release of classified and unclassified information that supports potential foreign involvement and foreign sales. Since preparation of this section requires a joint effort involving program management, security, intelligence, and designated disclosure authority personnel, it may be a task for the Research and Technology Protection Working-level Integrated Product Team.

When the TA/CP is prepared in the early stages of program protection planning, emphasis should be placed on describing the value of the technology and systems in terms of military capability, the economic competitiveness of the U.S. industrial base and technology, susceptibility to compromise, foreign availability, and likely damage in the event of compromise.

This assessment should result in a conclusion on whether a cooperative program, co-production, or foreign sale will result in clearly defined operational or technological benefits to the United States, and whether these benefits would outweigh any damage that might occur if there should be a compromise or unauthorized transfer. Specific reasons must be provided.

This assessment should identify and explain any critical capability, information, or technology that must be protected. It may reveal that an adjustment to program phasing is necessary so critical information is released only when absolutely necessary. It should identify any CPI that may not be released due to the impact on the system's combat effectiveness. Additionally, it will identify the need for special security requirements such as a program-specific security plan to govern international involvement. The assessment should also evaluate the risk of compromise, based on the capability and intent of foreign participants or purchasers to protect the information, and the susceptibility of the system to compromise if not protected.

Finally, the assessment should discuss any known foreign availability of the information, system, or technology involved; previous release of the same or similar information, system, or technology to other countries; and, when foreign involvement or sales are recommended, its release to other participants.

Control Plan. The fourth section, together with the technology assessment, provides the basis for guidance on negotiating technical and security aspects of the program, and development of disclosure guidelines for subsequent sales and foreign participation in the program.

The Control Plan should describe actions that are to be taken to protect U.S. interests when foreign involvement or sales are anticipated. Those actions should be specific and address specific risks, if any, as discussed in the technology assessment. Actions might include withholding certain information, stringent phasing of releases, or development of special security requirements.

The plan should also identify any design or engineering changes that may be necessary or desirable to ensure the protection of CPI. The plan should describe how security provisions of an agreement and/or applicable regulations are to be applied to the specific program, agreement, or sale.

In preparation of the Control Plan, special consideration should be given to the export restrictions on sensitive technologies and materials amplified in DoD Instruction S-5230.28 (This website is not authorized to post classified documents. Authorized users may contact the OPR: USD(AT&L), 703-697-0016) and the National Disclosure Policy Committee's Policy Statement on "Foreign Release of Low Observable and Counter Low Observable Information and Capabilities (U)".

Delegation of Disclosure Authority Letter (DDL). The program manager must prepare a DDL as part of a recommendation for foreign involvement, disclosure of the program to foreign interests, request for authority to conclude an international agreement, or a decision to authorize foreign sales. NOTE: The DDL is not releasable to Foreign Nationals.

The DDL should provide detailed guidance on releasability of all elements of the system, to include its technology and associated information. The SCG will be consulted during the preparation of the DDL to establish its classification.

The Program Manger (PM) develops the DDL in accordance with DoD Directive 5230.11 enclosure 4. The applicable designated disclosure authority should agree with its content. The DDL is provided to the Milestone Decision Authority and the Office of the Under Secretary of Defense (Policy) (USD(P)) for approval at each milestone. Until the DDL has been approved by the originating activity's designated disclosure authority, the Milestone Decision Authority, and the Office of the USD(P), there should be no promise to release, nor should there be actual release of, sensitive information or technology.

8.4.9. Contracting and Resources

8.4.9. Contracting and Resources

Program protection planning may be outsourced and included in a contract. That contract activity may include initial program and system evaluation as well as program protection planning that leads to specific Research and Technology Protection countermeasures. Early planning is necessary to ensure that funds are programmed and budgeted to provide timely required contract support.

Program protection activities should begin prior to contract award. Delaying the process may result in safeguards being difficult to accomplish or being omitted from contracts. The program's underpinning inherited or determined Critical Program Information should be factored into the program's overall acquisition strategy. The program manager is responsible for this planning and should prepare a budget for all security costs within the Planning, Programming, Budgeting, and Execution process and the program's Acquisition Program Baseline. It is more cost effective for security to be "baked in" early rather than "bolted on" later.

8.4.9.1. Early Coordination

As discussed in section 8.4.2, Research and Technology Protection (RTP) is a subject for early coordination by the program manager's staff and contracting personnel to ensure contractual documents contain essential protection requirements. Early coordination is fundamental for having adequate coverage in contractual documents and to thus avoid additional and unnecessary costs due to late application of RTP requirements. The expected range of protection requirements and projected resources required should be estimated to ensure research and acquisition planning documents address RTP. RTP is also a subject for early coordination by Designated Disclosure Authority personnel.

8.4.9.2. Pre-Contract Award

The pre-award phase includes pre-solicitation, solicitation, source selection evaluation, and other pre-award activities.

Acquisition organizations generally have local instructions and related checklists to aid the program management staff in completing the actions necessary to arrive at a legal and successful contract award. Such instructions and checklists should be written and reviewed to ensure they address program protection activities and requirements.

The program manager (PM) should define program protection requirements early enough to be included in the draft request for proposal (RFP).

- The initial program management staff, with the assistance of the program protection point of contact, provides the responsible contracting office with information describing the nature and extent of program protection requirements that apply to the contemplated contract and estimates for the resources necessary to contractually execute the program. (See the information listed in subsection 8.4.6)
- The PM includes a program protection section in the RFP and should ensure that the appropriate Federal Acquisition Regulation and/or Defense Federal Acquisition Regulation Supplement clauses have been activated.

Once the proposals are received in response to the RFP, they will be evaluated using specified source selection criteria. The resulting evaluation should address the proposed ways of satisfying program protection requirements. The evaluation should also consider the cost to execute each proposed approach to satisfy the contractor portion of the Program Protection Plan. An RTP specialist should be available to assist in the source selection process when proposals are required to address program protection requirements.

Approaches in the selected contractor's proposal documents should be incorporated into the contract. Action should be taken to ensure RTP provisions in the proposal are fully implemented by the prime contract.

The PM should require the contractors to coordinate with the program office staff and counterintelligence support staff, all proposals to market or otherwise obtain a commercial

export license to sell portions of the system being acquired or like systems to foreign countries. The PM should formalize this requirement in all Statements of Work for acquisition systems. A lack of coordination by the contractors may result in inadvertent transfer of critical military technology to unauthorized foreign nationals.

8.4.9.3. Post Contract Award

It is not unusual for contract modifications to be made reflecting fiscal or other program changes. As with pre-award actions, the program manager (PM) should ensure that the program office Research and Technology Protection (RTP) representative works with the program management staff and the contracting officer if RTP changes are required.

A primary post award activity is "baselining" the contract. RTP actions are addressed in this activity and, if applicable, identified as a reportable item in the baseline. When used, the contractor Program Protection Implementation Plan forms a principal source for the contract RTP baseline.

The contracting officer representative (COR) is formally identified during post award activities and becomes the focal point, along with the PM, for administering contract requirements, including RTP. The COR and the PM need to understand how RTP is important to successful achievement of protecting the program cost, schedule, and performance objectives. The COR should discuss the security requirements with the Designated Disclosure Authority.

8.4.9.4. Contractor Performance Monitoring

The contracting officer representative (COR), the Program Manager (PM), and the contracting officer (CO) are key to ensuring that RTP requirements are accomplished, particularly if there are any modifications to the contract. The RTP point of contact (POC) should monitor performance and schedule of RTP activities. As part of the program manager staff, the RTP POC works through the PM, COR, and CO in accomplishing RTP goals. Any proposed contract modifications regarding foreign involvement should also be discussed with the Designated Disclosure Authority.

Planning for performance monitoring begins with RFP activities, pre-award issues, and continues with the contract baselining and any necessary re-baselining.

The contract baseline, once documented, will be the prime contractor performance measurement tool. That baseline is compared with periodic performance reports that address work accomplished as well as costs incurred and related task funding. When the work breakdown structure is developed, any RTP action identified in the statement of work, preliminary acquisition planning activities, or the RFP, is identified as a "reportable item"

8.4.9.5. Contractor Costs

To properly support contract activities, Research and Technology Protection (RTP) costs are identified as part of the initial program definition and structuring. Those cost estimates are then used in the early contract development process, starting with drafting of the Request for Proposal.

Cost estimates are identified by category (i.e., personnel, products, services, equipment) to include any information systems requirements. Within each category of RTP costs, the items are further identified by security discipline.

Costs for implementing industrial security are included in the overhead portion of contractor costs. DoD security countermeasures are typically included in level-of-effort costs for DoD agencies. These costs should not be included in the Program Protection Plan since they are not additive costs to the acquisition program. The baseline for standard security actions is determined before identifying program-specific RTP costs.

RTP costs for implementing foreign disclosure and/or national disclosure policies are also identified by the categories listed in the paragraphs above.

8.4.9.6. Providing Documentation to Contractors

The program manager, in coordination with the Research and Technology Protection (RTP) point of contact and the contracting officer, determines when prime contractors, and subcontractors supporting the RTP effort, need access to Critical Program Information documentation. If a foreign contractor is involved, the Designated Disclosure Authority must participate in the coordination.

When a contractor is to be granted access to classified information, sensitive information, controlled unclassified information, For Official Use Only information, export-controlled data, or unclassified technical data, the contract will provide authorization for access to contractor facilities by the responsible government industrial security office (Defense Security Service or the DoD Component-cognizant security authority). That authorization is necessary to permit surveys, inspections, advice or assistance visits, or inquiries, which are necessary to ensure protection of sensitive information and implementation of RTP activities at prime, subcontractor, and/or vendor facilities.

Whenever possible, threat information (i.e., Counterintelligence Assessment) is shared with the cognizant contractor Facility Security Officer to ensure their understanding of the threat.

8.4.9.7. Support from Cognizant Government Industrial Security Offices

The contract DD Form 254, "DoD Contract Security Classification Specification," should specifically identify Research and Technology Protection (RTP) assessments and reviews to be

conducted by the responsible government industrial security office (e.g., Defense Security Service (DSS)). The program manager should complete the DD 254 to reflect RTP protection measures and requirements. A copy of the DD 254 should be provided to the cognizant government security office (i.e., the appropriate DSS field office) so they may assist in RTP protection efforts. Organizations responsible for RTP reviews should:

- Conduct or participate in reviews and assistance visits at contractor facilities and contractor activities at government facilities. Reviews at contractor facilities in the United States assess compliance with contractually-imposed RTP measures, when contract provisions authorize such reviews and visits.
- Disseminate evaluation reports to appropriate acquisition program officials (e.g., Program Executive Officers, program managers, user organization officials). Unless specifically prohibited, the program manager provides reports to appropriate contractor personnel.
- The program manager should also assure that DSS also receives a copy of those elements of the PPP related to its assigned responsibilities at the facility. In such cases, DSS should also received distribution of the involved PPP components if otherwise distributed separately, as well as their updates and related information. This includes such items as the Control Plan, the CI Analysis of Critical Program Information, Technology Targeting Risk Assessment, Counterintelligence Support Plan, Security Classification Guide, Information Exchange Agreements, and Program Protection Implementation Plan.

8.4.10. Research and Technology Protection (RTP) Costing and Budgeting

8.4.10. Research and Technology Protection (RTP) Costing and Budgeting

Ultimately, the success of an acquisition program will depend on protecting the research and technology upon which the acquisition is based. RTP requirements should be incorporated into initial program funding and subsequent budget submissions to ensure adequate resources are committed at program initiation.

When RTP professionals are part of the program costing and budgeting processes, RTP requirements can be addressed during programming and budgeting cycles.

8.4.10.1. Research and Technology Protection (RTP) Costing

Program resource managers are responsible for developing a Work Breakdown Structure (WBS) and Cost Analysis Requirements Description (CARD) as part of the overall costing process. The CARD is developed in concert with the WBS and serves as the costing portion of the WBS.

Costs for material, personnel/labor, training, etc., are incorporated into a requirements document to define overall RTP costs. Security, counterintelligence, and intelligence professionals should be integrated into the program costing process at the earliest opportunity.

A separate WBS category provides managers with visibility into RTP costs and actual funding available to support the RTP effort. A separate WBS category is recommended for RTP requirements such as anti-tamper, system security engineering, information assurance, and the Program Protection Implementation Plan.

8.4.10.2. Research and Technology Protection (RTP) Budgeting

Once RTP cost requirements are properly estimated and documented, the next step in the process is their submission and validation as part of the program budgeting process. All RTP costing requirements are coordinated with the program resource manager who prepares budget submissions to the program manager.

Often, a validation board is assembled to review program costing requirements. This board validates the cost (verifies the methodology used to project the costs) and prioritizes program cost requirements. When RTP cost proposals are submitted, RTP professionals should be present to support these proposals to the validation board. RTP professionals should serve as advisors to the program manager for RTP costs coming from other organizations or from contractors.

Once a program budget is approved and the RTP requirement funded, establishing a separate RTP funding line item could be useful in tracking funds that are distributed to support RTP requirements.

RTP points of contact who manage funding and/or the implementation of the Program Protection Implementation Plan are required to annually update their funding requirements and contribute to the overall program budget submission process. RTP costs will be validated each year.

8.4.11. Execution of the Program Protection Plan (PPP)

8.4.11. Execution of the Program Protection Plan (PPP)

The program manager has the primary responsibility for PPP execution. Specific functions and actions may also be assigned to supporting security, counterintelligence (CI), and intelligence organizations, as well as supporting acquisition organizations and defense contractors. Proper PPP execution depends on allocation of resources for planned Research and Technology Protection (RTP) countermeasures and communication of the RTP countermeasures plan to

applicable contractors, as well as to acquisition, security, CI, and intelligence activities supporting the program.

8.4.11.1. Distribution of the Program Protection Plan (PPP)

Once the PPP is approved, the program manager (PM) ensures all activities that are assigned Research and Technology Protection (RTP) actions in the PPP receive a copy of the approved plan or those portions pertaining to their tasks. Organizations that should be considered for PPP distribution include the following:

- Program contractors having Critical Program Information (CPI) under their control.
- Responsible government industrial security offices (i.e., Defense Security Service offices supporting the program at contractor sites covered by the PPP and/or the PPIP).
- DoD test ranges and centers applying CPI countermeasures
- Counterintelligence activities supporting program sites having CPI countermeasures applied.

If the PM decides to limit distribution of the entire PPP, then, as a minimum, the CPI and RTP countermeasures portions should be distributed to the appropriate organizations.

8.4.11.2. Assessment of Program Protection Plan (PPP) Effectiveness

The program manager, assisted by security and counterintelligence activities, assesses PPP effectiveness, and the research and technology protection countermeasures prescribed therein, as part of the normal program review process. Such assessments are planned considering the overall program schedule, the time-phased arrival or development of Critical Program Information at specific locations, and the schedule to revise the PPP.

8.5. Specialized Protection Processes

8.5.1. System Security Engineering

8.5.1.1. General

If the program manager decides to use system security engineering (SSE) it can be the vehicle for integrating research and technology protection into the systems engineering process. Systems engineering activities prevent and/or delay exploitation of Critical Program Information in U.S. defense systems and may include anti-tamper activities (see section 8.5.3). The benefit of SSE is derived after acquisition is complete by mitigation of threats against the system during deployment, operations, and support. SSE may also address the possible capture of the system by the enemy during combat or hostile actions.

8.5.1.2. System Security Engineering (SSE) Planning

The program manager's (PM's) System Engineering Plan (SEP) is the top-level management document used to describe the required systems engineering tasks. The System Security Management Plan (SSMP) is a detailed plan outlining how the SSE manager and the contractors will implement SSE, and may be part of the SEP.

The SSMP, prepared by the PM, establishes guidance for the following tasks:

- Analysis of security design and engineering vulnerabilities; and
- Development of recommendations for system changes, to eliminate or mitigate vulnerabilities through engineering and design, any characteristics that could result in the deployment of systems with operational security deficiencies.

The SSMP is applicable to the acquisition of developmental or existing systems or equipment.

MIL-HDBK-1785 establishes the formats, contents, and procedures for the SSMP. Data Item Description, DI-MISC-80839, SSMP, is applicable.

A System Security Engineering Working Group (SSEWG) defines and identifies all SSE aspects of the system, develops SSE architecture, reviews the implementation of the architecture, and

participates in design validation. The SSEWG is formed as early in the acquisition process as possible, but not later than the Technology Development phase of the acquisition. The SSEWG is comprised of acquisition program office personnel; supporting counterintelligence, intelligence, and security personnel; system user representatives; and other concerned parties. The SSEWG provides recommendations to the PM.

8.5.1.3. System Security Engineering (SSE) Process

SSE supports the development of programs and design-to-specifications providing life-cycle protection for critical defense resources. Activities planned to satisfy SSE program objectives are described in the System Security Management Plan (SSMP).

SSE secures the initial investment by "designing-in" necessary countermeasures and "engineering-out" vulnerabilities, and thus results in saving time and resources over the long term. During the system design phase, SSE should identify, evaluate, and eliminate (or contain) known or potential system vulnerabilities, spanning the life cycle from system deployment through system demilitarization.

The SSE process defines the procedures for contracting for an SSE effort and an SSMP. Implementation requires contractors to identify operational vulnerabilities and to take action to eliminate or minimize associated risks.

Contract Data Item Descriptions and Contract Data Requirements Lists may be tailored to the acquisition program to obtain contractor-produced plans or studies that satisfy specific program needs.

8.5.1.4. Military Handbook 1785

MIL-HDBK-1785 contains procedures for contracting an SSE effort and an SSMP. The format and contents are outlined in the appropriate Data Item Descriptions listed in MIL-HDBK-1785.

The proponent for the handbook is Commander, Naval Air Systems Command, ATTN: AIR-7.4.4., 22514 McCoy Road, Unit 10, Patuxent River, MD 20670-1457.

8.5.1.5. Security Engineering for International Programs

System Security Engineering should include an assessment of security criteria that sets limits for international cooperative programs, direct commercial sales, and/or foreign military sales cases. From this assessment, engineering and software alternatives (e.g., export variants, anti-tamper provisions) should be identified that would permit such transactions.

8.5.2. Counterintelligence Support Plan (CISP)

8.5.2. Counterintelligence Support Plan (CISP)

The CISP defines specific counterintelligence (CI) support to be provided to the research, development, test and evaluation (RDT&E) facility or acquisition program and provides the servicing CI personnel with information about the facility or program being supported.

- A tailored CISP is developed for every DoD RDT&E activity and for each DoD acquisition program with identified Critical Program Information (CPI);
- RDT&E site directors, security managers, and supporting CI organizations are responsible for developing a CISP for each RDT&E facility;
- Program managers (PMs) and their supporting security and CI organizations are responsible for developing a CISP for each acquisition program with CPI. The CPI will be listed in the CISP;
- The CISP is signed by local CI and site management personnel, the PM, and the local Defense Security Service representative, as appropriate. The CISP will specify which of the CI services will be conducted in support of the facility or program, and will provide the CI personnel with information about the program or facility to help focus the CI activities. A copy of the signed plan is provided to the DoD Component CI headquarters;
- The CISP will be reviewed annually, or as required by events. It will be used as the baseline for any evaluation of the program or facility and its supporting CI program; and
- Any updated CISP is redistributed to those providing support.

8.5.2.1. Counterintelligence (CI) Actions at Research, Development, Test and Evaluation (RDT&E) Activities

Component CI agencies have identified a core listing of CI services that are recommended for each CI Support Plan (CISP):

- If there is Critical Program Information (CPI) at a RDT&E site, the site director-approved CISP is provided to the DoD Component CI specialists working at the RDT&E site;
- If there is CPI at a RDT&E site, the program manager (PM)-approved CISP is provided to the DoD Component CI specialists working at the site and will become an annex to the site CISP;
- If CPI is identified at a DoD contractor facility, the PM, CI specialist, the Defense Security Service CI specialist, and the contractor develop a CISP annex to define CI support to the contractor; and
- If RDT&E site management identifies CPI requiring specialized CI support beyond what is covered in the project or program CISP, that additional support is documented as an annex to the site CISP.

DoD Component CI personnel keep the project or PM CI point of contact (POC) informed of threat and other information that could adversely impact CPI. The CI POC is responsible for keeping the PM or site director apprised of current CI activities.

When more than one DoD Component CI agency has an interest at the same RDT&E site or contractor facility, teaming, and cooperation should occur at the lowest possible organizational level. If a conflict occurs that cannot be resolved by the DoD Components, information on the conflict is sent to the Deputy Undersecretary of Defense (Counterintelligence and Security), in the office of the Under Secretary of Defense (Intelligence), for review and resolution.

8.5.2.2. Counterintelligence (CI) Support to Acquisition Programs

DoD Component CI organizations should identify a CI specialist to acquisition program managers with Critical Program Information (CPI). The CI specialist should:

- Participate in the Research and Technology Protection (RTP) Working-level Integrated Product Team that develops the Program Protection Plan and is responsible for developing the CI Support Plan (CISP) and obtaining the Counterintelligence Analytical product for the program;
- Ensure CI RTP requirements flow to CI and security personnel at locations where the CPI is used, handled, stored, or tested;
- Ensure the program manager and the program office staff are aware of current threat information; and
- Provide specialized CI support to all locations pursuant to the CISP.

Field CI personnel should:

- Provide CI RTP support when the weapons system or other platform becomes operational for as long as CPI is designated; and
- Provide CI support for as long as the CPI is so designated.

8.5.3. Anti-Tamper

8.5.3.6. Guidelines for Anti-Tamper (AT) Disclosure

8.5.3.1. General

- Program managers should develop and implement anti-tamper (AT) measures to protect Critical Program Information (CPI) in U.S. defense systems developed using co-development agreements; sold to foreign governments; or no longer within U.S. control (e.g., theft, battlefield loss). AT techniques may be applied to system performance, materials, hardware, software, algorithms, design, and production methods, or maintenance and logistical support. Although protective in nature, AT is not a substitute for program protection or other required security measures;
- AT protects leading edge CPI on weapon systems, training devices, and maintenance support equipment, and adds longevity to a critical technology by deterring reverse engineering. AT also provides time to develop more advanced technologies to ensure previously successful hostile exploitation of a defense system does not constitute a threat to U.S. military forces and capabilities. Although AT may not completely defeat exploitation, it will make hostile efforts time-consuming, difficult, and expensive;
- AT considerations and design needs to be initiated as early as possible during program development, preferably in the program concept refinement and technology development phases, in conjunction with the identification of program CPI:
    - AT is also applicable to DoD systems during a Pre-Planned Product Improvement upgrade or a deployed system technology insertion; and
    - Additionally, AT should be specifically addressed in all transfer or sales of fielded systems and in direct commercial sales to foreign governments if those systems have CPI to protect.
- AT resource requirements may affect other aspects of a program, to include end item cost, schedule, and performance;
- AT also involves risk management. A decision not to implement AT should be based on the risk of the asset falling out of US control, operational impact if the CPI is lost, as well as on acquisition risks, to include: AT technical feasibility, cost, system performance, and scheduling impact;
- The DoD Anti-Tamper Executive Agent (ATEA) resides with the Department of the Air Force, which is responsible for:
    - Managing AT Technology Development;
    - Implementing Policy;
    - Developing an AT databank / library;
    - Developing a Technology Roadmap;
    - Providing Proper Security Mechanisms; and
    - Conducting AT Validation.
- The DoD ATEA has established a network of DoD Component AT points of contact (POCs) to assist program managers in responding to AT technology and/or implementation questions. Additionally, DoD Component AT POCs and at the AT field Office have created a shared common databank of AT related infomration; and

- Since AT is a systems engineering activity, AT is strengthened when integrated into a program sub-system(s), and is more cost effective when implemented at program onset.

8.5.3.2. Application of Anti-Tamper (AT)

- With the aid of the DoD AT Component POC, the program manager should determine the criticality of the CPI found within the program. This can be found in the DoD ATEA's Guidelines document. In addition to criticality of CPI, the CPI exposure must also be determined. With the exposure and criticality determined, the appropriate AT protection level for each CPI is indicated in the AT Guidelines document. The evaluation may indicate there is no requirement to apply AT techniques. However, a final decision should not be made until completing thorough operational and acquisition risk analyses;
- AT applicability should be assessed for each major modification or Pre-Planned Product Improvement upgrade to the production system and for any export of fielded systems or direct commercial sale. It is feasible that AT may be inserted into the modified or upgraded systems when protection is required. AT may be discontinued when it is determined the technology no longer needs protection; and
- The PM recommendation whether or not to implement AT should be approved by the Milestone Decision Authority and documented in the Program Protection Plan.

8.5.3.3. Anti-Tamper (AT) Implementation

- The program manager (PM) should document the analysis and recommendation in the classified AT plan (an annex to the Program Protection Plan (PPP)), of whether or not to use AT measures. The PPP with the AT annex should be included in the submission for Milestone B, and updated for Milestone C. The AT Executive Agent, or any DoD Component-appointed AT Agent, provides an evaluation of the AT plan and a letter of concurrence to the Milestone Decision Authority;
- The AT classified annex to the PPP contains AT planning. The planning detail should correspond to the acquisition phase of the program;
- The AT annex includes, but is not limited to, the following information:
    - Identification of the critical technology being protected and a description of its criticality to system performance;
    - Foreign Teaming and foreign countries / companies participating;
    - Threat assessment and countermeasure attack tree;
    - AT system level techniques and subsystem AT techniques investigated;
    - System maintenance plan with respect to AT;
    - Recommended solution to include system, subsystem and component level;
    - Determination of how long AT is intended to delay hostile or foreign exploitation or reverse-engineering efforts;
    - The effect that compromise would have on the acquisition program if AT were not implemented;

    - The estimated time and cost required for system or component redesign if a compromise occurs;
    - The PM recommendation and the Milestone Decision Authority decision on AT; and
    - The program AT point of contact.
- AT is reflected in system specifications and other program documentation; and
- AT, whether implemented or not, should be a discussion item during Milestone B, Milestone C (Low-Rate Initial Production), and Full-Rate Production Decision Reviews:
    - At Milestone B, the PM should address AT in conceptual terms and how it is to be implemented. Working AT prototypes, appropriate to this stage of program development, should be demonstrated. Deliverables at Milestone B include: a list of critical technologies/information; a Counterintelligence analysis of CPI; a list of identified vulnerabilities; identified attack scenarios; impacts if exploited; available AT techniques; and a preliminary AT Plan. These deliverables are submitted and incorporated into the AT Annex of the PPP; and
    - At Milestone C, the PM should fully document AT implementation. Deliverables at Milestone C include: all deliverables from Milestone B and any updates; an analysis of AT methods that apply to the system, including cost/benefit assessments; an explanation of which AT methods will be implemented; and a plan for verifying and validating (V&V) AT implementation. These deliverables are submitted and incorporated into the AT annex of the PPP. Testing during developmental test and evaluation and operational test and evaluation is highly encouraged for risk reduction.

8.5.3.4. Anti-Tamper (AT) Verification and Validation (V&V)

AT implementation is tested and verified during developmental test and evaluation and operational test and evaluation.

The program manager (PM) develops the validation plan and provides the necessary funding for the AT V&V on actual or representative system components. The V&V plan, which is developed to support Milestone C, is reviewed and approved by the AT Executive Agent, or any DoD Component-appointed AT Agent, prior to milestone decision. The program office conducts the V&V of the implemented AT plan. The AT Executive Agent witnesses these activities and verifies that the AT plan is implemented into the system and works according to the AT plan. The PM and the AT Executive Agent may negotiate for parts of the system that have undergone AT measures to be tested at the AT Executive Agent's laboratories for further analysis. The validation results are reported to the Milestone Decision Authority.

8.5.3.5. Sustainment of Anti-Tamper (AT)

AT is not limited to development and fielding of a system. It is equally important during life-cycle management of the system, particularly during maintenance.

AT measures should apply throughout the life cycle of the system. Maintenance instructions and technical orders should clearly indicate that AT measures have been implemented; indicate the level at which maintenance is authorized; and include warnings that damage may occur if improper or unauthorized maintenance is attempted. To protect Critical Program Information, it may be necessary, as prescribed by the Delegation of Disclosure Authority Letter, to limit the level and extent of maintenance a foreign customer may perform. This may mean that maintenance involving the AT measures will be accomplished only at the contractor or U.S. Government facility in the U.S. or overseas. Such maintenance restrictions may be no different than those imposed on U.S. Government users of AT protected systems. Contracts, purchase agreements, memoranda of understanding, memoranda of agreement, letters of agreement, or other similar documents should state such maintenance and logistics restrictions. When a contract that includes AT protection requirements and associated maintenance and logistics restrictions also contains a warranty or other form of performance guarantee, the contract terms and conditions should establish that unauthorized maintenance or other unauthorized activities:

- Should be regarded as hostile attempts to exploit or reverse engineer the weapon system or the AT measure itself; and
- Should void the warranty or performance guarantee.

The U.S. Government and U.S. industry should be protected against warranty and performance claims in the event AT measures are activated by unauthorized maintenance or other intrusion. Such unauthorized activities are regarded as hostile attempts to exploit or reverse engineer the system or the AT measures.

8.5.3.6. Guidelines for Anti-Tamper (AT) Disclosure

The fact that AT has been implemented in a program should be unclassified unless the appropriate original classification authority of the DoD Component, in consultation with the program Milestone Decision Authority, decides that the fact should be classified. Please refer to the AT security classification guide for further information.

The measures used to implement AT will normally be classified, including any potential special handling caveats or access requirements. The AT implementation on a program should be classified from SECRET / US ONLY (minimum) to SECRET / SAR per the AT security classification guide. Classified AT information, including information concerning AT techniques, should not be disclosed to any unauthorized individual or non-U.S. interest pursuant to decisions made by appropriate disclosure authorities.

Disclosure decisions should take into account guidance and recommendations from the program Original Classification Authority, in consultation with the program Milestone Decision Authority, and the Under Secretary of Defense for Acquisition, Technology and Logistics. The program Milestone Decision Authority coordinates all foreign disclosure releases involving AT with the cognizant designated disclosure authority and security assistance office, as appropriate.

An exception to National Disclosure Policy may be warranted for co-development programs, foreign military sales, or direct commercial sales.

8.5.4. Information Assurance (IA)

All information systems (including network enclaves) storing, processing, or transmitting Critical Program Information (CPI) must comply with the requirements of DoD Directive 8500.01E, "Information Assurance (IA)," and implement the appropriate IA controls from DoD Instruction 8500.2, "Information Assurance Implementation." Accordingly, these systems will be accredited in accordance with DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)." The DIACAP establishes a standard process, set of activities, general task descriptions, and a management structure to certify and accredit information technology systems throughout the system life cycle. A product of the DIACAP, the System Security Authorization Agreement (SSAA), documents the agreement between the project manager, the Designated Approval Authority (DAA), the Certification Authority, and the user representative concerning schedule, budget, security, functionality, risk, and performance issues. Applicable SSAAs will be included as annexes to the Program Protection Plan (PPP). Associated costs will be recorded in the PPP by fiscal year. For information systems where the program office is not the owner of the system but simply a user of the system, the PPP should include a copy of the system's Approval to Operate issued by the system DAA.

It is important to differentiate between the implementation of IA with regards to program support systems processing CPI, as opposed to the implementation of IA in the system being acquired. For example, a hypothetical acquisition program office acquiring a new weapons system (or automated information system) may have an information system that supports the storing, processing and transmitting of CPI. The IA requirements and certification and accreditation requirements for that support system are totally separate and distinct from those of the weapons system being acquired. Chapter 7, *Acquiring Information Technology and National Security Systems*, provides specific guidance on the identification and implementation of IA requirements for all systems being acquired.

8.5.5. Horizontal Analysis and Protection

8.5.5. Horizontal Analysis and Protection

The objective of horizontal analysis and protection activities is to ensure consistent, cost-effective application of similar Research and Technology Protection safeguards for similar Critical Program Information throughout DoD.

- DIA conducts horizontal analysis to determine whether similar technologies are being used in different programs;
- Program Managers, Program Executive Officers, and Milestone Decision Authorities should assist in these analyses to ensure that similar technologies are safeguarded with the same level of protection, (i.e., horizontal protection); and
- The Under Secretary of Defense for Intelligence, the Under Secretary of Defense for Acquisition, Technology and Logistics, and the Director, Operational Test and Evaluation provide oversight of the effectiveness of horizontal analysis and protection as outlined in DoD Instruction 5200.39.

8.5.5.1. Horizontal Analysis

The DIA-conducted horizontal analysis should address the following:

- System enabling technologies (Critical Program Information (CPI)) and their additional applications, whether for similar or dissimilar tasks;
- Research and Technology Protection safeguards planned or provided;
- Intelligence estimates of competitive foreign acquisition efforts; and
- Reports of completed investigations of compromises, espionage cases, and other losses.

DoD Components should establish processes that support horizontal analysis and protection activities. DoD Components should:

- Identify system enabling technologies and their additional applications, whether for similar or dissimilar tasks;
- Review security classification guides of existing programs or projects when developing a Counterintelligence Support Plan or Program Protection Plan (PPP) to determine classification of similar technologies used in other programs or under development; and
- Catalogue, analyze, group, and correlate protection requirements within approved PPPs for CPI involving similar enabling technologies. Provide the data collected to the DIA for their use.

8.5.5.2. Horizontal Protection

DIA, through the Defense Counterintelligence and HUMINT Center, will provide their analysis report to the site director for emerging technologies and/or to the program manager (PM) for their application within an acquisition program. Site directors or PMs should ensure their respective Counterintelligence Support Plan and Program Protection Plan are modified when required based upon results of the horizontal analysis.

DIA, through the Defense Counterintelligence and HUMINT Center will coordinate all reported or discovered discrepancies with the appropriate DoD Components for resolution at the lowest possible organizational level.

When necessary, DIA, through the Defense Counterintelligence and HUMINT Center will report unresolved or inconsistent applications of Research and Technology Protection safeguards to the Under Secretary of Defense for Acquisition, Technology and Logistics, the Director, Operational Test and Evaluation, and the Under Secretary of Defense for Intelligence for resolution. Copies of these reports will be provided to the DoD Inspector General.

8.5.5.3. Reporting Requirements

Compromise of Critical Program Information will be reported through counterintelligence channels to DIA, through the Defense Counterintelligence and HUMINT Center and the Under Secretary of Defense for Intelligence, in accordance with DoD Instruction 5240.04.

8.5.6. Research and Technology Protection (RTP) Assessments and Inspections

8.5.6. Research and Technology Protection (RTP) Assessments and Inspections

Periodic assessments and inspections of RTP activities (encompassing all DoD research, development, test and evaluation (RDT&E) budget categories) are necessary to ensure effective RTP is being planned and implemented. The DoD Component responsible for the RDT&E site or the acquisition program is responsible for these assessments and inspections (DoD Instruction 5200.39).

8.5.6.1. Assessments

DoD Components periodically assess and evaluate the effectiveness of Research and Technology Protection implementation by Research, Development, Test and Evaluation (RDT&E) site directors and program managers as well as the support provided by security, intelligence, and counterintelligence to RDT&E sites and acquisition programs with Critical Program Information.

8.5.6.2. Inspections

The DoD Inspector General (IG) has established a uniform system of periodic inspections, using the existing DoD Components' inspection processes for Research, Development, Test and

Evaluation (RDT&E) sites, to ensure compliance with directives concerning security, research and technology protection (RTP), and counterintelligence practices.

The DoD IG has developed RTP inspection guidelines for use by DoD and DoD Component Inspectors General to enhance consistent application of directives that apply to RTP directives and related issuances.

DoD Component IGs conduct periodic inspections, using the DoD IG inspection guidelines, of RDT&E sites and acquisition programs for compliance with RTP directives. These inspections assess program manager compliance with section 8.4.11.2, *Assessment of PPP Effectiveness*. Participating Inspectors General may modify or customize the DoD IG inspection guidelines to account for Military Department-specific approaches to security, technology protection, and counterintelligence.

The DoD IG conducts periodic audits of DoD Component IG inspections for compliance with RTP directives and related issuances.

DEFENSE ACQUISITION GUIDEBOOK
Chapter 9 -- Test and Evaluation (T&E)

9.0. Overview

9.0.1. Purpose

This chapter will help the acquisition and Test and Evaluation (T&E) communities develop a robust strategy for T&E to support program and warfighter decisions, including the assessment of operational effectiveness and suitability.

9.0.2 Contents

Section 9.1 provides an introduction of general topics associated with Test and Evaluation (T&E).

Section 9.2 then presents an overview of the T&E support and oversight provided by the Offices of the Director, Operational Test and Evaluation (DOT&E); and the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)).

The next few sections focus on specific types of T&E:

Section 9.3 - Developmental Test and Evaluation (DT&E);

Section 9.4 - Operational Test and Evaluation (OT&E); and

Section 9.5 - Live Fire Test and Evaluation (LFT&E).

Section 9.6 covers T&E planning and specifically addresses the Test and Evaluation Strategy (TES) and Test and Evaluation Master Plan (TEMP).

Section 9.7 covers T&E Reporting.

Section 9.8 presents examples of best practices.

Section 9.9 covers special topics. And

Section 9.10 closes with details of preparing a TEMP.

Throughout this chapter, the terms developmental and operational should be interpreted as broad statements of types of testing or evaluation, and not as the testing controlled by a particular organization.

9.1. Introduction to Test and Evaluation (T&E)

9.1.5. Test and Evaluation (T&E) Working Integrated Product Team (T&E WIPT)

9.1. Introduction to Test and Evaluation (T&E)

The fundamental purpose of T&E is to provide knowledge to assist in managing the risks involved in developing, producing, operating, and sustaining systems and capabilities. T&E provides knowledge of system capabilities and limitations to the acquisition community for use in improving the system performance, and the user community for optimizing system use and sustainment in operations. T&E enables the acquisition community to learn about limitations (technical or operational) of the system under development, so that they can be resolved prior to production and deployment.

Developmental Test and Evaluation (DT&E) supports the following:

- The systems engineering process to include providing information about risk and risk mitigation;
- Assessing the attainment of technical performance parameters;
- Providing empirical data to validate models and simulations; and
- Information to support periodic technical performance and system maturity evaluations.

Operational Assessments (OAs) are conducted early in a program to provide insight into potential operational problems and progress toward meeting desired operational effectiveness and suitability capabilities.

OT&E is conducted to evaluate system operational effectiveness, suitability, and survivability in support of the full-rate production decision review.

LFT&E permits the evaluation of system survivability in the context of vulnerability to realistic threat munitions and/or system lethality against realistic threat targets.

This chapter provides DoD guidance to Program Managers (PMs) for use in planning and executing an integrated and robust T&E program within their programs. The PM, in coordination with representatives of the test communities (to include Developmental Test (DT), Operational Test (OT), contractor, and others as appropriate (i.e., Joint Interoperability Test Command (JITC), Defense Information Systems Agency (DISA))) develops an integrated test strategy for the program. An integrated test strategy strives to ensure the collaborative test planning and execution of developmental (both contractor and government) and operational test events to provide shared data in support of independent analysis, evaluation, and reporting by all stakeholders.

Testing should be event driven within the program's overall acquisition strategy, and allow for a realistic period of time to accomplish the planned test events, evaluations, and report preparation. Test planners will ensure the exit criteria (e.g., required test results) of integrated test events will satisfy the objectives of each test community (DT, OT, JITC) participating in the event. The PM,

through the T&E Working-Level Integrated Product Team (T&E WIPT), must ensure that the DT&E program is robust in order to achieve a successful OT&E outcome. The T&E WIPT should include representatives from the Program Management Office, T&E agencies, operational users, the Office of the Secretary of Defense (OSD) staff, DoD Component staffs, the intelligence community, and other agencies as necessary to assist in this task. The PM is required to develop metrics (hardware and software), in the form of T&E success criteria and OT&E entrance criteria (in consultation with the Operational Test Agency), to use in monitoring program maturity and to support decisions to progress through the development cycle.

9.1.1. Evolutionary Acquisition

The Test and Evaluation (T&E) strategy of a system acquired using evolutionary acquisition should allow for adequate T&E of each increment intended for fielding. In general, T&E that has previously confirmed the effectiveness and suitability of a previous increment need not be repeated in its entirety to confirm that the subsequent increment still provides those mission capabilities. However, regression testing to reconfirm previously tested operational capabilities and/or suitability might be required if the subsequent increment introduces a significantly changed hardware or software configuration, or introduces new functions, components, or interfaces that could reasonably be expected to alter previously confirmed capabilities. The requirement for regression testing is a topic for T&E Working-level Integrated Product Team discussion and resolution. Evolutionary acquisition approaches do not eliminate the need for the Initial Operational Test and Evaluation required by statute.

9.1.2. Relationship of the Joint Capabilities Integration and Development System (JCIDS) to Test and Evaluation (T&E)

JCIDS defines mission capability gaps, overlaps, and redundancies that could result in the acquisition of a new materiel solution. The requirements process supports the acquisition process by providing validated capabilities and associated performance criteria to be used as a basis for acquiring the right systems. T&E will assess whether new or modified systems deliver their intended capability within the applicable functional capabilities area. There will be a need to consider realistic test environments, including joint mission and joint test environments, to assess an individual system's contribution to joint mission capability. The JCIDS documents of interest to T&E are the Initial Capabilities Document, the Capability Development Document, the Capability Production Document, and the Concept of Operations (CONOPS) for the system under development.

There are many different types of CONOPS prepared to address strategic and tactical employment and support concepts as well as other aspects of mission accomplishment. All of these CONOPS should be used by the T&E community to understand how and in what context the system will be employed. For T&E purposes, CONOPs should be used to understand how and in what environments the system will be employed and tested.

9.1.2.1. Initial Capabilities Document (ICD)

The ICD defines the capability gap(s) in terms of the functional area, the relevant range of military operations, desired effects, time, Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, or Facilities, and constraints. It proposes a recommended approach that best satisfies the desired capability. It supports the work required to refine the initial concept, and should form the end-state objectives for the initial Test and Evaluation (T&E) strategy development documented in the Test and Evaluation Strategy. Because the ICD statement of desired capabilities is broad and not system-specific, the T&E strategy may also be a broad, general discussion of capability risk areas, knowledge required for major decisions, and a rough order of magnitude, or range of test program size and scope options. (See the JCIDS Manual)

9.1.2.2. Capability Development Document (CDD)

The CDD specifies the operational requirements for the system that will deliver the capability that meets operational performance criteria specified in the Initial Capabilities Document. It outlines a militarily useful increment of capability with its own set of attributes and performance values (i.e., thresholds and objectives). As the CDD is going through the Joint Requirements Oversight Council approval process prior to program initiation, the T&E Working-level Integrated Product Team (T&E WIPT) updates the test and evaluation (T&E) strategy using the system-specific details in the CDD. The CDD provides the Key Performance Parameters and Key System Attributes that provide a focus for the T&E program. The T&E strategy gains details (specific, desired, operational capabilities; T&E events (Developmental Test and Evaluation, Operational Test and Evaluation, and Live Fire Test and Evaluation) adding to the broad, initial T&E strategy; Critical Operational Issues; refining the management structure and composition of the T&E WIPT; identifying resource requirements more precisely; etc.) that refines the scope and size of the planned T&E program, and permits a better estimate of the T&E resources and costs. Because the CDD normally is not approved until around the time of Milestone B, the T&E WIPT will most likely have to work from a draft version, to prepare the Test and Evaluation Master Plan prior to the Milestone B decision. (See the JCIDS Manual)

9.1.2.3. Capability Production Document (CPD)

The final step in the capabilities refinement process is CPD development, with the refined operational capabilities and system performance expected from the production articles. The CPD is used by the T&E Working-level Integrated Product Team to update the Test and Evaluation Master Plan for the Milestone C decision and for subsequent updates later in Production and Deployment, such as the full rate production decision review. At Milestone C, the technical testing begins to focus on production testing, such as Production Qualification Testing, to demonstrate performance of the production system in accordance with the contract. Operational testing focuses on evaluating the Low-Rate Initial Production system's operational effectiveness, suitability, survivability, and mission capability. (See the JCIDS Manual)

9.1.3. Network-Centric Operations

Implementation of the Department's transformation strategy, calling for shifting to an information-age military, will result in fewer platform-centric and more network-centric military forces. This requires increased information sharing across networks. The network-centric concept applies to a DoD enterprise-wide information management strategy that includes not only military force operations but also all defense business processes, such as personnel actions, fuel purchases and delivery, commodity buying, deployment and sustainment activities, acquisition and development. Key tenets of the strategy include: handle information only once, post data before processing it, users access data when it is needed, collaborate to make sense of data, and diversify network paths to provide reliable and secure network capabilities.

The shift away from point-to-point system interfaces to network-centric interfaces brings implications for the Test and Evaluation (T&E) community. The challenge to the test community will be to represent the integrated architecture in the intended operational environment for test. Furthermore, the shift to network-centric capabilities will evolve gradually, no doubt with legacy point-to-point interfaces included in the architectures. Program managers, with their Program Executive Officer's support, are strongly encouraged to work with the operating forces to integrate operational testing with training exercises, thereby bringing more resources to bear for the mutual benefit of both communities. It is imperative that the T&E community engages the user community to assure that test strategies reflect the intended operational and sustainment/support architectures and interfaces within which the intended capabilities are to be tested and evaluated.

9.1.4. Integrated Testing

Integrated Testing is defined by OSD Memo, "Definition of Integrated Testing," dated 25 April 2008.

> *"the collaborative planning and collaborative execution of test phases and events to provide shared data in support of independent analysis, evaluation, and reporting by all stakeholders, particularly the developmental (both contractor and government) and operational test and evaluation communities."*

Integrated testing is not an event or separate test phase, nor is it a new type of test. Integrated testing is a process intended to result in resource efficiencies (time, money, people, and assets) and an enhanced data set for separate evaluations. For example, the data from an integrated test could be used by the contractor for design improvements, by the developmental evaluators for risk assessments, and the operational evaluators for operational assessments. However, integrated testing does not replace or eliminate the need for dedicated Initial Operational Test and Evaluation required by 10 USC 2399, "Operational Test and Evaluation of Defense Acquisition Programs" and DoD Instruction 5000.02.

The goal of integrated testing is to conduct a seamless test program that produces credible qualitative and quantitative data useful to all evaluators, and to address developmental, sustainment, and operational issues. Integrated testing allows for the collaborative planning of test events, where a single test point or mission can provide data to satisfy multiple objectives, without compromising the test objectives of participating test organizations. Test points in this context, mean a test condition denoted by time, three-dimensional location and energy state, and system operating configuration, where a pre-planned test technique is applied to the system under test and the response(s) are observed and recorded. Integrated testing is not just concurrent or combined Developmental Test (DT) and Operational Test (OT), where both DT and OT test points are interleaved on the same mission or schedule. Integrated testing focuses the entire test program (contractor test, Government DT, Live Fire Test, and OT) on designing, developing, and producing a comprehensive plan that coordinates all test activities to support evaluation results for decision makers at required decision reviews.

Integrated testing must be embedded in the test and evaluation (T&E) strategy, although most of the effort takes place during the detailed planning and execution phases of a test program. The foundation of the integrated test strategy should be based upon an Evaluation Framework as discussed in Section 9.6.2.2. It is critical that all stakeholders understand what evaluations are required to assess risks, assess maturity of the system and to assess the operational effectiveness, operational suitability and survivability/lethality. The "end state" of what will be evaluated must be defined up front so all stakeholders are working toward the same goal. Once this is accomplished, an integrated test program can be developed that generates the data required to conduct the evaluations.

One method used to develop integrated testing is to perform a mission analysis by decomposing the Critical Operational Issues (COIs) into tasks and subtasks. Being derived from the capability requirements documents and the concept of operations, the COIs are a starting point in developing the test program. Breaking the COIs into tasks and subtasks will ensure system designers, developmental testers, operational testers and user representatives are all in agreement concerning the missions, tasks, and defined capabilities. There is no single implementation of integrated testing that will be optimum for all programs, but planning and conducting the test program in a collaborative manner will result in a more effective and efficient test effort.

Once the COIs and tasks/subtasks are understood, the Critical Technical Parameters, Measures of Effectiveness, and Measures of Suitability can be developed and presented in the Evaluation Framework, thus ensuring direct traceability and linkage of system characteristics, key performance parameters/key system attributes, specifications, and user requirements, to a mission or missions. Such a structured approach also ensures that all test activities are necessary, duplication is eliminated, and that no areas are missing in the overall T&E effort.

For integrated testing to be successful, it is important that the pedigree of the data be understood and maintained. The pedigree of the data refers to accurately documenting the configuration of the test asset and the actual test conditions under which each element of test data was obtained. The T&E Working-level Integrated Product Team (T&E WIPT) (see below) plays an important

role in maintaining the data pedigree within the integrated test process for a program. The T&E WIPT establishes agreements between the test program stakeholders, regarding roles and responsibilities in not only implementing the integrated test process, but also in developing and maintaining data release procedures, and data access procedures or a data repository, where all stakeholders will have access to test data for separate evaluations.

9.1.5. Test and Evaluation (T&E) Working Integrated Product Team (T&E WIPT)

To develop a strategy and guide the execution of the test and evaluation (T&E) program, a Program Manager (PM) should charter a T&E WIPT. It should be established as early as possible during Material Solutions Analysis, and it should be chaired by a program office representative. Membership should consist of all stakeholder organizations that require test data for Developmental Test, Operational Test or any other required certifications, and the user representative. For programs on the OSD T&E Oversight List, OSD T&E oversight agencies should be included. PMs should also consider forming lower level functional working groups, who report to the T&E WIPT, whose focus is on specific areas such as integrated test planning (see above), reliability scoring, modeling and simulation development, and Verification, Validation, and Accreditation, threat support, etc. The charter should be developed early to, as a minimum, identify the responsibilities of the participating membership, and to describe the process by which the T&E WIPT will resolve issues. Working tools of the T&E WIPT include draft and final statements of desired capabilities, budget documentation, threat documentation, Technology Development Strategy, acquisition strategy, T&E strategies (T&E Strategy and T&E Master Plan), and detailed evaluation plans.

9.2. OSD Responsibilities

9.2. OSD Responsibilities

There are two organizations within the OSD that have policy and oversight responsibilities for test and evaluation (T&E). They are

1. Director, Operational Test and Evaluation (DOT&E): the Principal Staff Assistant and advisor to the Secretary of Defense for the responsibilities and functions described below;
2. Director, Developmental Test and Evaluation (DDT&E) within the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)):

responsible for developing DT&E policies, practices, and procedures; and provides direct interface with program managers on DT&E program support.

These offices share or coordinate on the following responsibilities:

- Provide advice and make recommendations to the Secretary and Deputy Secretary of Defense and the USD(AT&L) and support Overarching Integrated Product Teams (OIPTs) and Defense Acquisition Boards/Information Technology Acquisition Boards for programs on the OSD T&E Oversight List ;
- Develop, in consultation with the DoD Components, the OSD T&E Oversight List;
- Ensure the adequacy of test and evaluation strategies and plans for programs on the OSD T&E Oversight List;
- Attend systems engineering technical reviews ;
- Monitor and review DT&E, Operational Test and Evaluation (OT&E), and Live Fire Test and Evaluation events of oversight programs;
- Participate in the operational test readiness process by providing recommendations about a system's readiness for OT&E;
- Provide independent performance, schedule, and T&E assessments to the Defense Acquisition Executive Summary process; and
- Provide representatives to the T&E WIPT of oversight programs to assist PMs in developing their strategy and preparing a T&E Strategy /T&E Master Plan .

In addition to the T&E policy and oversight organizational elements, the Test Resource Management Center (TRMC), under the USD(AT&L), has responsibility for ensuring the adequacy of test resources in the Major Range and Test Facility Base.

9.2.1. Specific Responsibilities of Director, Operational Test and Evaluation (DOT&E)

Specific responsibilities of the DOT&E are listed in DoD Directive 5141.02, "Director of Operational Test and Evaluation". For additional information on the DOT&E office, visit the DOT&E website.

The DOT&E shall:

a. Perform the duties prescribed in, and as limited by, 10 USC 139 and 10 USC 2399.
b. Prescribe policies and procedures for the conduct of Live Fire Test and Evaluation (LFT&E).
c. Issue guidance to and consult with the Heads of the DoD Components with respect to LFT&E and related required facilities and resources.
d. Advise the DoD Executive Agent for Space and the acquiring Military Department on test and evaluation (T&E) of DoD Space Major Defense Acquisition Programs and other space programs designated for T&E oversight in support of DoD Directive 3100.10.

e. Designate, for the Secretary of Defense, those covered systems and major munitions or missile programs that are deemed covered product improvement programs subject to the requirements of 10 USC 2366.
f. For the Secretary of Defense, prepare reports to Congress as required by 10 USC 2366, paragraph (d).
g. Provide reports, as deemed necessary, to the Secretary and Deputy Secretary of Defense, the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), and other appropriate officials in support of system acquisition reviews.
h. Monitor and advise the Secretary of Defense concerning:
    1. The capability and resources of the operational test agencies to adequately plan, execute, and report on Operational Test and Evaluation (OT&E).
    2. DoD and DoD Component management of, and investment in, targets and threat surrogates used for OT&E and LFT&E to ensure operational realism.
    3. The OT&E and LFT&E of functional capability area roadmaps.
i. Manage the following:

    1. The efforts to improve interoperability and information assurance through the operational evaluation of the systems under oversight and major exercises conducted by the Combatant Commands and the Military Departments.
    2. The Joint Test and Evaluation (JT&E) Program.
    3. The Joint Live Fire Program.
    4. The Center for Countermeasures.
    5. The activities of the Joint Aircraft Survivability Program.
    6. The activities of the Joint Technical Coordinating Group for Munitions Effectiveness and produce the Joint Munitions Effectiveness Manual.
    7. The activities of the T&E Threat Resource Activity.
    8. The Target Management Initiative project.
    9. Such other programs that are established by the DOT&E within the resources provided by the Secretary of Defense.
j. In support of the Under Secretary of Defense for Intelligence, monitor and advise on the development of the Information Operations Range and infrastructure. Establish supporting policies and procedures and oversee events that are executed on the Information Operations Range.
k. Prioritize threat system simulation development projects to be initiated under the Central Test and Evaluation Investment Program (CTEIP), subject to availability of funds.
l. Provide the co-chair for the Resource Enhancement Project (REP) working group. Prioritize candidate projects to be initiated in the REP under the CTEIP.
m. Oversee the implementation of the testing in a joint environment roadmap.
n. Provide support to the Director, Joint Improvised Explosive Device Defeat Organization, consistent with DoD Directive 2000.19E.
o. Assist the Chairman of the Joint Chiefs of Staff in efforts to ensure the expected joint operational mission environment, mission level measures of effectiveness, and key performance parameters are specified in Joint Capabilities Integration and Development

System documents in terms that are verifiable through testing or analysis in support of CJCS Instruction 3170.01.

p. Oversee and assess operational capability demonstrations conducted by the Missile Defense Agency consistent with DoD Directive 5134.9.
q. Establish policy on the verification, validation, and accreditation of models and simulations used in support of OT&E and LFT&E in compliance with this Instruction.
r. Oversee the International T&E (IT&E) Program for the Secretary of Defense.

    1. Approve activities authorized under international agreements for reciprocal use of ranges and resources, cooperative T&E programs, project equipment transfers, cooperative project personnel and familiarization visits, and international test operations procedures (ITOPS).
    2. Chair the IT&E Steering Committee for ITOPS.

s. Oversee and prescribe policy, as appropriate, to ensure protection of human subjects and adherence to ethical standards are adequately addressed and verified in OT&E and LFT&E, in support of DoD Directive 3216.02.
t. Promote coordination, cooperation, and mutual understanding within the Department of Defense and between the Department of Defense and other Federal Agencies; State, local, and foreign governments; and the civilian community with regard to DOT&E matters.
u. Perform such other duties as the Secretary or Deputy Secretary of Defense may prescribe.

Relationships

a. *DOT&E.* In the performance of assigned responsibilities and functions, the DOT&E shall:
    1. Report directly to the Secretary of Defense.
    2. Serve as a permanent member of the Deputy Secretary of Defense-chartered T&E Executive Agent Board of Directors.
    3. Chair the Senior Advisory Council and the Executive Steering Group for the JT&E Program.
    4. Coordinate with the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) to facilitate efficient development and sustainment of operational test and training infrastructure and to promote combined testing and training events, in support of DoD Directive 1322.18 and DoD Directive 3200.15.
    5. Use existing systems, facilities, and services of the Department of Defense and other Federal Agencies, when possible, to avoid duplication and achieve maximum efficiency and economy.
    6. Coordinate with the Director, Test Resource Management Center (TRMC), through the USD(AT&L), on all T&E facility and resource matters as prescribed herein that affect TRMC responsibilities, as specified in DoD Directive 5105.71.
    7. Coordinate proposed international agreements supporting the IT&E Program with the Director, International Cooperation, under the USD(AT&L).

8. Coordinate, with the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO), the Military Departments, the Combatant Commands, and the National Security Agency, the planning and conduct of information assurance and interoperability assessments conducted in conjunction with Military Department and Combatant Command major exercises.
9. Coordinate and exchange information with other DoD officials exercising collateral or related responsibilities and functions.

b. *Other OSD officials and the Heads of the DoD Components.* The other OSD officials and the Heads of the DoD Components shall coordinate with the DOT&E on all matters under their purview related to the authorities, responsibilities, and functions assigned in this Directive. The Heads of the DoD Components, as appropriate, shall report promptly to the DOT&E all activities affecting the resources and facilities used for OT&E and LFT&E.
c. *Secretaries of the Military Departments.* The Secretaries of the Military Departments shall perform their duties as prescribed in 10 USC 139. Additionally, the Secretaries of the Military Departments shall report promptly to the DOT&E the results of all LFT&E events conducted by the Military Departments and on all studies conducted by the Military Departments in connection with LFT&E activities.
d. *Director, MDA.* The Director, MDA, shall perform duties as prescribed in 10 USC 139.
e. *IG, DoD.* The IG, DoD, shall perform duties as prescribed in 10 USC 2399.

Authorities

Under the authority vested in the Secretary of Defense, and subject to his/her authority, direction, and control, and in accordance with DoD policies and issuances, the DOT&E is hereby delegated authority to exercise, within assigned responsibilities and functions, all authority of the Secretary of Defense derived from statute, Executive order, or interagency agreement, except where specifically limited by statute or Executive order to the Secretary of Defense. The DOT&E is hereby delegated authority to:

a. Comply with requests from Congress for information relating to T&E in the Department of Defense.
b. Co-approve the DoD Test and Evaluation Master Plan (TEMP), T&E Strategy (TES), and T&E portions of integrated program management documents with the USD(AT&L) for major and other designated defense acquisition programs, and with the ASD(NII)/DoD CIO for major and other designated automated information systems. Approve the TEMP, TES, or T&E portions of the integrated program management documents for programs that are solely under DOT&E oversight. Approve Test Plans for operational test events of acquisition systems under DOT&E oversight.
c. Approve LFT&E strategies and, if developed in support of waivers of full-up system-level live fire testing, alternative LFT&E strategies.
d. Act for the Secretary of Defense regarding cooperative agreements for reciprocal use of test facilities under 10 USC 2350l.

e. Determine the quantity of articles to be procured for operational testing for systems on the OSD T&E oversight list.
f. Co-chair, with the USD(P&R), the Defense Test and Training Steering Group.
g. Issue, in DoD Instructions, DoD policy within the responsibilities, functions, and authorities assigned herein, including authority to identify collateral responsibilities of OSD officials and the Heads of the DoD Components. Such Instructions shall be fully coordinated in accordance with DoD Instruction 5025.01. This authority may not be redelegated. Further, in areas of assigned responsibilities and functions, the DOT&E has authority to issue other DoD Instructions, DoD Manuals, and one-time directive-type memorandums, consistent with DoD Instruction 5025.01, that implement policy approved by the Secretary of Defense. Instructions to the Military Departments shall be issued through the Secretaries of the Military Departments. Instructions to the Combatant Commands shall be communicated through the Chairman of the Joint Chiefs of Staff.
h. Communicate with the Heads of the DoD Components, as necessary, to carry out assigned responsibilities and functions, including the transmission of requests for advice and assistance. Communications to the Military Departments shall be through the Secretaries of the Military Departments, their designees, or as otherwise provided in law or directed by the Secretary of Defense in other DoD issuances. Communications to the Commanders of the Combatant Commands, except as provided for in memorandums of agreement concerning personnel support, shall be transmitted through the Chairman of the Joint Chiefs of Staff.
i. Obtain reports and information, consistent with DoD Instruction 8910.01, as necessary in carrying out assigned responsibilities and functions.
j. Establish arrangements for DoD participation in non-defense governmental programs for which the DOT&E is assigned primary cognizance.
k. Communicate with other Government officials, representatives and members of the Legislative Branch, members of the public, and representatives of foreign governments, as appropriate, in carrying out assigned responsibilities and functions. Communications with representatives of the Legislative Branch shall be coordinated with the Assistant Secretary of Defense for Legislative Affairs or the Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense, as appropriate, and be consistent with the DoD Legislative Program, as appropriate.

9.2.2. Specific Responsibilities of the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L))

The Office of the Director, Developmental Test & Evaluation (DDT&E), under the Deputy Under Secretary of Defense for Acquisition and Technology has Developmental Test and Evaluation responsibilities. The DDT&E responsibilities are described on their webpage. Another office, the Test Resource Management Center (TRMC), is a field activity reporting directly to the USD(AT&L) and has primary responsibility for the planning and assessment of the adequacy of the Major Range and Test Facility Base to provide adequate testing in support of development, acquisition, fielding, and sustainment of defense systems. Specific responsibilities of the TRMC are listed in DoD Directive 5105.71, "DoD Test Resource Management Center."

9.2.3. OSD Test and Evaluation (T&E) Oversight List

The Director, Operational Test and Evaluation, and the Director, Developmental Test & Evaluation (DDT&E), jointly, and in consultation with the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)), the DoD Component T&E executives, and other offices as appropriate, publish an annual OSD T&E Oversight List. Programs on the list can be designated for Developmental Test and Evaluation, Operational Test and Evaluation, and/or Live Fire Test and Evaluation oversight. Any program, regardless of Acquisition Category (ACAT) level, can be considered for inclusion, and can be added to or deleted from the list at any time during the year. OSD criteria for determining whether or not a program should be on formal T&E oversight includes:

- ACAT level;
- Potential for becoming an acquisition program (such as the Technology Projects identified in Enclosure 3 of DoD Instruction 5000.02 or a pre-Major Defense Acquisition Program);
- Stage of development or production;
- Whether program is subject to Defense Acquisition Executive Summary reporting;
- Congressional and DoD interest;
- Programmatic risk (cost, schedule, performance);
- Past history of the developmental command with other programs;
- Relationship with other systems as part of a system-of-systems; and
- Technical complexity of system.

9.3. Developmental Test and Evaluation (DT&E)

9.3.1. Developmental Test and Evaluation (DT&E) Guidelines

A well planned and executed DT&E program supports the acquisition strategy and the systems engineering process, providing the information necessary for informed decision-making throughout the development process and at each acquisition milestone. Developmental Test (DT) provides the verification and validation of the systems engineering process and must provide confidence that the system design solution is on track to satisfy the desired capabilities. The test and evaluation (T&E) strategy should be consistent with and complementary to the System Engineering Plan and acquisition strategy. The T&E team should work closely with the Program Manager (PM) and the system design team to facilitate this process. Rigorous component and sub-system DT&E enables performance capability and reliability improvements to be designed into the system early. DT&E events should advance to robust, system-level and system-of-systems level T&E, to ensure that the system has matured to a point where it can enter production, and ultimately meet operational employment requirements.

Robust DT&E reduces technical risk and increases the probability of a successful program. During early DT&E, the prime contractor will focus testing on technical contract specifications. To ensure that the systems engineering verification and validation relates back to user required capabilities, it is appropriate for government testers to observe the contractor testing, conduct additional T&E, and, when appropriate, facilitate early user involvement and contribution in the design and test processes. The PM's contract with industry must support an interface between government testers and users with the contractors' testing. The OSD "Incorporating Test and Evaluation into Department of Defense Acquisition Contracts" provides additional guidance on contract-related issues for the successful solicitation, award, and execution of T&E related aspects of acquisition contracts. Items such as commercial-off-the-shelf, non-developmental items, and Government-off-the-shelf products, regardless of the manner of procurement, must undergo DT&E to verify readiness to enter IOT&E, where operational effectiveness, suitability, and survivability for the intended military application are confirmed. Programs should not enter IOT&E unless the DoD Components are confident the system is effective, suitable, and survivable. In addition, the government's DT&E results will be reported at each program milestone, to provide knowledge to reduce the risk in those acquisition decisions.

PMs are required to develop a T&E strategy that meets the following objectives:

- Serve as the basis for T&E budgetary estimates identified in the Cost Analysis Requirements Description (required by DoD 5000.4-M).
- Integrate DT and Operational Test (OT) objectives into a single test strategy to maximize efficiencies during test execution while minimizing test resource requirements;
- Perform verification and validation in the systems engineering process;
- Be event-driven, rather than schedule-driven;
- Identify technological capabilities and limitations of alternative concepts and design options under consideration to support cost-performance tradeoffs. The intent is to avoid locking onto one solution too early;
- Identify and describe design technical risks. The T&E strategy should naturally flow from the systems engineering processes of requirements analysis, functional allocation,

and design synthesis. For further explanation of this systems engineering flow-down, refer to section 4.2 of this Guidebook;

- Stress the system under test to at least the limits of the Operational Mode Summary/Mission Profile, and for some systems, beyond the normal operating limits to ensure the robustness of the design. This testing will reduce risk for performance in the expected operational environments;
- Assess technical progress and maturity against Critical Technical Parameters (CTPs), including interoperability, documented in the TEMP. As part of an event-driven strategy, the use of success criteria is a suggested technique with which program managers can meet this requirement. Success criteria are intermediate goals or targets on the path to meeting the desired capabilities. There are two uses of success criteria. First, they can be used to assess technical progress and maturity against CTPs. Second, they can be used as metrics to assess successful completion of a major phase of developmental testing, such as a major phase of ground testing or of flight testing, and determine readiness to enter the next phase of testing, whether developmental or operational. In the case of operational testing, these success criteria are tantamount to IOT&E entrance criteria which are required for all operational tests. Technical parameters, such as levels of reliability growth or software maturity, increasing levels of system accuracy, mission processing timelines, can be used as success criteria to assess technical progress. Alternatively, in the case of an event success criterion such as completion of the first set of missile test firings, the criterion can be a specified level of success, such as a percentage of successful missile firings from this group. Failure to meet this criterion might cause the PM to decide on additional firings prior to transitioning to the next phase of testing. A PM can use a combination of both types of success criteria and tailor them to best fit the program's T&E strategy;
- Assess the safety of the system or item to ensure safe operation prior to IOT&E, other troop-supported testing, operational usage, and to support success in meeting design safety criteria. The intent is to ensure that developmental systems are sufficiently free of hazards to prevent injury to the typical users participating in IOT&E and fielding;
- Provide data and analytic support to the Milestone C decision to enter low-rate initial production (LRIP);
- Provide data and analytic support to certify the system ready for IOT&E. These data are provided in the DT&E report discussed below;
- Conduct Information Assurance (IA) testing on any system that collects, stores, transmits, and processes unclassified or classified information. The extent of IA testing depends upon the assigned Mission Assurance Category and Confidentiality Level. DoD Instruction 8500.2, "Information Assurance (IA) Implementation," mandates specific IA Control Measures that a system should implement as part of the development process.
- In the case of Information Technology (IT) systems, including National Security Systems (NSS), support the DoD Information Assurance Certification and Accreditation Process and Joint Interoperability Certification process;
- Discover, evaluate, and mitigate potentially adverse electromagnetic environmental effects (E3);

- Support joint interoperability assessments required to certify system-of-systems interoperability;
- Conduct an independent assessment of compliance factors established by the Office of the USD(C) for financial management, enterprise resource planning, and mixed financial management systems;
- Demonstrate the maturity of the production process through Production Qualification Testing of Low-Rate Initial Production assets prior to full-rate production. The focus of this testing is on the contractor's ability to produce a quality product, since the design testing should already have finished.
- Demonstrate performance against threats and their countermeasures as identified in the DIA or component-validated threat document. Any impact on technical performance by these threats should be identified early in technical testing, rather than in operational testing where their presence might have more serious repercussions; and
- Ensure the T&E strategy is aligned with and supports the approved acquisition strategy, so that adequate, risk-reducing T&E information is provided to support decisions.

In addition to the mandatory items above, the following three items are strongly recommended to ensure a robust T&E program:

- Utilize ground test activities, where appropriate, to include hardware-in-the-loop simulation, prior to conducting full-up, system-level testing, such as flight-testing, in realistic environments;
- To mitigate technical risk, the required assessment of technical progress should also include reliability, maintainability and supportability desired capabilities, and technical and manufacturing risks; and
- Assess system-of-systems Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance prior to OT&E to ensure that interoperability under loaded conditions will represent stressed OT&E scenarios.

9.3.2. Systems Engineering and Test and Evaluation (T&E)

Systems engineering is discussed in depth in Chapter 4 of this Guidebook. In essence, systems engineering is a process to transform required operational and sustainment capabilities into a system design solution. As the design solution evolves, a verification component of the systems engineering process must provide confidence that the design solution properly addresses the desired capabilities, as intended. T&E is the mechanism for accomplishing the verification loop in the systems engineering process and characterizing technical risk of achieving a proper final design solution.

9.3.3. Critical Technical Parameter (CTP) Development Process

Test and evaluation (T&E) programs will have hundreds or thousands of technical parameters that must be captured to support data analysis and evaluations; however, every technical

parameter is not a CTP. CTPs are measurable critical system characteristics that, when achieved, enable the attainment of desired operational performance capabilities. They are not simply a restatement of the key performance parameters and/or key system attributes. Each CTP must have a direct or significant indirect, correlation to key Capability Development Document/Capability Production Document operational requirements, required system specifications or concept of operations-related operational need. CTPs should be focused on critical design features or risk areas (e.g., technical maturity; Reliability, Availability, and Maintainability issues; cost) that if not achieved or resolved during development, will preclude delivery of required operational capabilities. CTPs are likely to evolve/change as the system matures during Engineering and Manufacturing Development. Existing CTPs should be resolved and new ones may be identified as the system progresses during development. Any CTPs not resolved prior to entering Low-Rate Initial Production should be identified and an action plan established to resolve them prior to the Full-Rate Production Decision Review.

The lead government T&E engineer is the responsible agent for the CTP process. The Chief Engineer or Technical Director is responsible for defining the CTPs. Once the CTPs are identified, the developmental evaluators identify the appropriate test methodologies (e.g., modeling and simulation, System Integration Lab (SIL), bench test) to obtain the data needed to evaluate the performance of the system and resolve the CTPs. Developmental evaluators use their evaluation of CTP maturity to inform the PM that the system is on (or behind) the planned development schedule or will likely (or not likely) achieve an operational capability. CTP evaluation results should be used as entry or exit criteria for major developmental test phases. If the CTPs are satisfactorily resolved, the system continues into the next phase of development. If not, action needs to be taken by the Program Manager to modify the system design or obtain relief from the required capability.

9.3.4. Modeling and Simulation (M&S) in Test and Evaluation (T&E)

For T&E, the appropriate application of M&S is an essential tool in achieving both an effective and efficient T&E program. T&E is conducted in a continuum of live, virtual, and constructive environments. DoD Components have guidelines for use of M&S in acquisition, especially T&E. These guidelines are intended to supplement other such resources. The program manager should have an M&S subgroup to the T&E Working-level Integrated Product Team (T&E WIPT) that develops the program's M&S strategy that should be documented in the program's Systems Engineering Plan and the Test and Evaluation Strategy/ Test and Evaluation Master Plan. Some DoD components require planning for M&S to be documented in a separate M&S Support Plan. This M&S strategy will be the basis for program investments in M&S. M&S should be planned for utility across the program's life cycle, modified and updated as required to ensure utility as well as applicability to all increments of an evolutionary acquisition strategy. A program's T&E strategy should leverage the advantages of M&S. M&S planning should address which of many possible uses of M&S the program plans to execute in support of T&E. Models and simulations can be used in planning to identify high-payoff areas in which to apply scarce test resources. Rehearsals using M&S can help identify cost effective test scenarios and reduce risk of failure.

During conduct of tests, M&S might provide adequate surrogates to provide stimulation when it is too impractical or too costly to use real world assets. This impracticality is particularly likely for capability testing or testing a system that is part of a system-of-systems, or for hazardous/dangerous tests or in extreme environments, or for testing the system's supportability. M&S can be used in post-test analysis to help provide insight, and for interpolation or extrapolation of results to untested conditions.

To address the adequacy and use of M&S in support of the testing process the program should involve the relevant operational test agency (OTA) in planning M&S to ensure support for both developmental test and operational test objectives. This involvement should begin in the early planning stages of the program.

An initial goal for the T&E WIPT is to assist in developing the program's M&S strategy by helping to integrate a program's M&S with the overall T&E strategy; plan to employ M&S tools in early designs; use M&S to demonstrate system integration risks; supplement live testing with M&S stressing the system; and use M&S to assist in planning the scope of live tests and in data analysis.

Another goal for the T&E WIPT is to develop a T&E strategy identifying how to leverage program M&S which could include how M&S will predict system performance, identify technology and performance risk areas, and support determining system effectiveness and suitability. For example, M&S should be used to predict sustainability or key system attribute drivers. The T&E WIPT should encourage collaboration and integration of various stakeholders to enhance suitability (see section 5.2.3).

A philosophy for interaction of T&E and M&S is to model-test-fix-model. Use M&S to provide predictions of system performance, effectiveness, suitability, and survivability and, based on those predictions, use tests to provide empirical data to confirm system performance and to refine and further validate the M&S. This iterative process can be a cost-effective method for overcoming limitations and constraints upon T&E. M&S may enable a comprehensive evaluation, support adequate test realism, and enable economical, timely, and focused test.

Computer-generated test scenarios and forces, as well as synthetic stimulation of the system, can support T&E by creating and enhancing realistic live test environments. Hardware-in-the-loop simulators enable users to interact with early system M&S. M&S can be used to identify and resolve issues of technical risk, that require more focused testing. M&S tools provide mechanisms for planning, rehearsing, optimizing, and executing complex tests. Integrated simulation and testing also provides a means for examining why results of a physical test might deviate from pre-test predictions. Evaluators use M&S to predict performance in areas that are impractical or impossible to test.

All M&S used in T&E must be accredited by the intended user (Program Manager or OTA). Accreditation can only be achieved through a robust verification, validation, and accreditation (VV&A) process, and an acknowledged willingness by the user to accept the subject M&S for

their application requirements. Therefore, the intended use of M&S should be identified early so that resources can be made available to support development and VV&A of these tools. The OTA should be involved early in this process so as to gain confidence in the use of M&S and possibly use them in support of operational testing. DoD Instruction 5000.61, "DoD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A)," provides further guidance on VV&A.

The following is provided to help the M&S subgroup to the T&E WIPT think through the planning process to best incorporate models and simulations into the testing process. Additional guidance for modeling and simulation is available in section 4.5.8 and in the "Guide for Modeling and Simulation for the Acquisition Workforce."

- Document the intended use of models and simulations:
  - Decisions that will rely on the results of the models and simulations
  - The test objectives/critical operational and sustainment issues the models and simulations will address
  - The requirements for the use of the models and simulations
  - Risk of use of models and simulations.
- Identify all models & simulations intended to support T&E including (but not limited to):
  - Type: live, virtual, and constructive simulations; distributed simulations and associated architecture; federates and federations; emulators; prototypes; simulators; and stimulators;
  - Suitability of model use: Legacy systems, new developments, and modified or enhanced legacy models & simulations;
  - Management of models and simulations: Developed in-house, Federally Funded Research and Development Centers, industry, academia, and other Federal or non-Federal government organizations;
  - Source: Commercial-off-the-shelf and government-off-the-shelf models and simulations;
  - Facilities: hardware-in-the loop, human-in-the-loop, and software-in-the-loop simulators; land-based, sea-based, air-and space-based test facilities;
  - Threat models, simulations, simulators, stimulators, targets, threat systems, and surrogates;
  - Synthetic countermeasures, test beds, environments, and battle spaces;
  - Models and simulations whether embedded in weapon systems, implemented as stand-alone systems, or integrated with other distributed simulations; and
  - Test assets, test planning aids, and post-test analysis tools that address other than real time characteristics.
- Infrastructure needed to conduct a (the) test(s) to include networks, integration software, and data collection tools.
  - Provide descriptive information for each model and simulation resource:
    - Title, acronym, version, date;
    - Proponent (the organization with primary responsibility for the model or simulation);

        - Assumptions, capabilities, limitations, risks, and impacts of the model or simulation;
        - Availability for use to support T&E; and
        - Schedule for obtaining.
- Identify the modeling and simulation data needed to support T&E:
    - Describe the input data the models and simulations need to accept;
    - Describe the output data the models and simulations should generate;
    - Describe the data needed to verify and validate the models and simulations; and
    - Provide descriptive information for each data resource:
        - Data title, acronym, version, date;
        - Data producer (organization responsible for establishing the authority of the data);
        - Identify when, where, and how data was or will be collected;
        - Known assumptions, capabilities, limitations, risks, and impacts;
        - Availability for use to support T&E; and
        - Schedule for obtaining.
- For each model and simulation and its data, describe the planned accreditation effort based on the assessment of the risk of using the model and simulation results for decisions being made.
    - Explain the methodology for establishing confidence in the results of models and simulations;
    - Document historical source(s) of VV&A in accordance with DoD Instruction 5000.61; and
    - Provide the schedule for accrediting prior to their use to support T&E.
- Describe the standards (both government and commercial) with which the models and simulations and associated data must comply; for example:
    - Information technology standards identified in the DoD Information Technology (IT) Standards Registry (DISR) (limited access);
    - Standards identified in the DoD Architecture Framework Technical Standards Profile (TV-1) and Technical Standards Forecast (TV-2);
    - Modeling & Simulation Standards and Methodologies (requires registration/login);
    - Data standards; and
    - VV&A standards:
        - IEEE Std 1516.4TM -2007, IEEE Recommended Practice for VV&A of a Federation—An Overlay to the High Level Architecture Federation Development and Execution Process;
        - IEEE Std 1278. 4TM -1997(R2002), IEEE Recommended Practice for Distributed Interactive Simulation - VV&A;
        - MIL-STD-3022 DoD Standard Practice for Model & Simulation VV&A Documentation Templates.

9.3.5. Mission-oriented Context

A mission-oriented context to T&E means being able to relate evaluation results to an impact on the warfighters' ability to execute their mission-essential tasks. Including mission context during test planning and execution provides for a more robust test environment, and allows for identification of design issues that may not be discovered in a pure developmental test environment. The results of testing in a mission-oriented context will allow these issues to be addressed earlier in the development phase of a component or system. Additionally, testing in a mission-oriented context will allow the developmental evaluators to predict system performance against the Critical Operational Issues (COIs) evaluated in Operational Test and Evaluation (OT&E).

Testing in a mission-oriented context will also allow the operational test agency (OTA) to participate earlier in the development cycle and use the results of integrated tests to make operational assessments. Integrated planning of tests is a key element in this process. This allows the data to be used by the developmental community to better predict system performance and allows the OTA to potentially reduce the scope of Initial Operational Test and Evaluation while still providing an adequate evaluation of the COIs.

9.3.6. System Readiness for Operational Test and Evaluation (OT&E)

9.3.6.1. Operational Test Readiness Process

The DoD Components should develop and institutionalize processes to determine a system's performance and readiness for operational assessments and tests. These processes should focus on ensuring that systems are in a realistic configuration and have demonstrated technical maturity under the expected operating conditions. Successful execution of these processes should enable the gathering of relevant and appropriate data, during integrated testing, to satisfy early operational test objectives prior to dedicated, operational testing.

9.3.6.2 System Readiness for IOT&E

For programs on the OSD T&E Oversight List for Operational Test and Evaluation (OT&E), the DoD Component Acquisition Executive (CAE) is required to evaluate and determine materiel system readiness for Initial Operational Test and Evaluation (IOT&E). The intent of this requirement is to ensure systems do not enter IOT&E before they are sufficiently mature. Scarce resources are wasted when an IOT&E is halted or terminated early because of technical problems with the system under test, problems that should have been resolved prior to the start of IOT&E.

Prior to the CAE determination of readiness for IOT&E, an independent Assessment of Operational Test Readiness (AOTR) will be conducted by DUSD(A&T) on all ACAT ID programs and special interest programs designated by the USD(AT&L). The AOTR will focus on the technical and materiel readiness of the program to proceed into IOT&E. Assessment results are based on capabilities demonstrated in DT&E and earlier Operational Assessments

(OA). A DT&E report of results and the progress assessment shall be provided to USD(AT&L) and DOT&E prior to the AOTR. That report can be a written document or a briefing to DOT&E and USD(AT&L) representatives, and should include the following: an analysis of the system's progress in achieving Critical Technical Parameters; satisfaction of approved IOT&E entrance criteria; a technical risk assessment; level of software maturity and status of software trouble reports; and predicted IOT&E results; including the impacts of any shortcomings on the system's expected performance during IOT&E. Provide the report at least 20 days prior to the CAE's determination of system readiness. This will allow OSD time to formulate and provide its recommendation to the CAE. All appropriate developmental and operational test and evaluation organizations should be invited to the IOT&E readiness review.

The goal of the AOTR is to assess the risk associated with the system's ability to meet operational suitability and effectiveness goals, identify system and subsystem maturity levels, assess programmatic and technical risk, and provide risk mitigation recommendations. The results of the AOTR will be provided to the USD(AT&L), DOT&E, and Component Acquisition Executive (CAE). The CAE shall consider the results of the AOTR prior to making a determination of materiel readiness for IOT&E.

9.4. Operational Test and Evaluation (OT&E)

9.4.1. Operational Test and Evaluation (OT&E) Guidelines

DoD Instruction 5000.02 lists mandatory elements of OT&E planning and execution. Other considerations are included here:

- The concept of early and integrated testing should emphasize prototype testing during system development and demonstration and early operational assessments (OAs) to identify technology risks and provide operational user impacts. Operational test agencies (OTAs) should maximize their involvement in early, pre-acquisition activities. The goal of integrated testing is to provide early operational insights during the developmental process. This early operational insight should reduce the scope of the integrated and

dedicated OT&E, thereby contributing to reduced acquisition cycle time and improved performance.

- Appropriate use of accredited models and simulation to support Developmental Test and Evaluation (DT&E), OT&E, and Live Fire Test and Evaluation (LFT&E) should be coordinated through the T&E Working-level Integrated Product Team (T&E WIPT).
- Planning should consider an integrated Developmental Test (DT), Operational Test (OT), and Live Fire (LF) approach. The integrated approach should not compromise either DT or OT objectives. Planning should provide for an adequate OT period and report generation, including the Director, Operational Test and Evaluation (DOT&E) Beyond-Low-Rate Initial Production (LRIP) Report to SecDef and Congress prior to the full-rate production decision.
- The DoD Component OTA is responsible for OT&E, including planning, gaining DOT&E plan approval, execution, and reporting.
- OT&E uses threat or threat representative forces, targets, and threat countermeasures, validated by the Defense Intelligence Agency or the DoD Component intelligence agency, as appropriate, and approved by DOT&E during the test plan approval process. DOT&E oversees threat target, threat simulator, and threat simulation acquisitions and validation to meet developmental, operational, and live fire test and evaluation needs.
- OT&E planning should consider modeling and simulation (M&S). Test planners should collaborate early with the Program Manager's (PM) M&S Proponent on the planned use of M&S to support or supplement their test planning or analyze test results. Where feasible, consideration should be given to the use or development of M&S that encompasses the needs of each phase of T&E. Test planners must coordinate with the M&S proponent/developer/operator to establish acceptability criteria required to allow verification, validation, and accreditation of proposed M&S. It is the responsibility of the PM's M&S Proponent to ensure verification and validation is conducted in a manner that supports accreditation of M&S for each test event/objective. Whenever possible, an OA should draw upon test results with the actual system, or subsystem, or key components thereof, or with operationally meaningful surrogates. When actual system testing is not possible to support an OA, such assessments may utilize computer modeling and/or hardware in the loop, simulations (preferably with real operators in the loop), or an analysis of information contained in key program documents. The Test and Evaluation Master Plan explains the extent of M&S supporting OT&E; if M&S is to be developed, resources must be identified and cost/benefit analysis presented.
- Naval vessels, the major systems integral to ship construction, and military satellite programs typically have development and construction phases that extend over long periods of time and involve small procurement quantities. To facilitate evaluations and assessments of system performance (operational effectiveness, suitability and mission capability), the program manager should ensure the independent OTA is involved in the monitoring of or participating in all relevant activity to make use of any/all relevant results to complete OAs. The OTA should determine the inclusion/exclusion of test data for use during OAs and determine the requirement for any additional operational testing needed for evaluation of operational effectiveness, suitability and mission capability.

- OTAs should participate in early DT&E and M&S to provide operational insights to the PM, the Joint Capabilities Integration and Development System process participants, and acquisition decision-makers.
- OT&E will evaluate information assurance (IA) on any system that collects, stores, transmits, or processes unclassified or classified information. This evaluation will include IA vulnerability and penetration testing.
- OT&E will evaluate potentially adverse electromagnetic environmental effects (E3) and spectrum supportability situations. Operational testers should use all available data and review DD Form 1494, "Application for Equipment Frequency Allocation," to determine which systems need field assessments. And,
- OT&E should take maximum advantage of training and exercise activities to increase the realism and scope of both the OT&E and the training, and to reduce testing costs.

9.4.2. Validation of Threat Representations (targets, threat simulators, or modeling and simulation (M&S))

To ensure test adequacy, operational testing should only incorporate validated, accredited threat representations unless coordinated with Director, Operational Test and Evaluation (DOT&E).

The recommended validation guidelines are:

- Threat representation validation supports the objective of ensuring that threat representations meet Developmental Test and Evaluation (DT&E) and Operational Test and Evaluation (OT&E) credibility requirements. Validation of threat representations is defined as "the baseline comparison of the threat to the threat representation, annotation of technical differences, and impact of those differences on testing."
- Validation of threat representations is typically conducted by the DoD Component responsible for the threat representation and culminates in a validation report which documents the results. DOT&E approves the DOD Component-validated reports.
- Only current, Defense Intelligence Agency- or DoD Component-approved threat data should be used in the validation report. Specifications pertaining to the threat representation should accurately portray its characteristics and may be obtained from a variety of sources including the developer and/or government-sponsored testing. For new developments, validation data requirements should be integrated into the acquisition process to reduce the need for redundant testing.
- Incorporation of an Integrated Product and Process Development (IPPD) process for new threat representation developments is recommended. The objective of the IPT is to involve DOT&E and its Threat Systems Office (TSO) early and continuously throughout the validation process. DoD Component organizations responsible for conducting threat representation validation should notify DOT&E of their intent to use an IPPD process and request DOT&E/TSO representation at meetings and reviews, as appropriate. The DOT&E representative will be empowered to provide formal concurrence or non-concurrence with these validation efforts as they are accomplished. After the IPPD

process, DOT&E will issue an approval memorandum, concurring with the threat representation assessment.

- When a Working-level Integrated Product Team is not used, draft threat representation validation reports should be forwarded to the TSO for review. TSO will provide recommendations for corrections, when necessary. Final reports are then submitted to the TSO for DOT&E approval.
- DOT&E approval confirms that an adequate comparison to the threat has been completed. It does not imply acceptance of the threat test asset for use in any specific test. It is the responsibility of the OTA to accredit the test resource for a specific test and for DOT&E to determine if the threat test resource is adequate.

These guidelines do not address the threat representation verification or accreditation processes. Verification determines compliance with design criteria and requires different methods and objectives. Accreditation, an OTA responsibility, determines the suitability of the threat representation in meeting the stated test objectives. The data accumulated during validation should be a primary source of information to support the accreditation process.

9.4.3. Evaluation of Test Adequacy

Operational Test and Evaluation adequacy encompasses both test planning and test execution. Considerations include the following:

- Realistic combat-like conditions
  - Equipment and personnel under realistic stress and operations tempo
  - Threat representative forces
  - End-to-end mission testing
  - Realistic combat tactics for friendly and enemy
  - Operationally realistic environment, targets, countermeasures
  - Interfacing systems
- Production representative system for Initial Operational Test and Evaluation
  - Articles off production line preferred
  - Production representative materials and process
  - Representative hardware and software
  - Representative logistics, maintenance manuals
- Adequate resources
  - Sample size
  - Size of test unit
  - Threat portrayal
- Representative typical users
  - Properly trained personnel, crews, unit
  - Supported by typical support personnel and support package
  - Missions given to units (friendly and hostile)

9.4.4. Evaluation of Operational Effectiveness

Operational effectiveness is the overall degree of mission accomplishment of a system when used by representative personnel in the environment planned or expected for operational employment of the system considering organization, training, doctrine, tactics, survivability, vulnerability, and threat.

The evaluation of operational effectiveness is linked to mission accomplishment. The early planning for the evaluation should consider any special test requirements, such as the need for large test areas or ranges or supporting forces, requirements for threat systems or simulators, new instrumentation, or other unique support requirements.

For weapon systems, integrate Live Fire Test and Evaluation (LFT&E) of system lethality into the evaluation of weapon system effectiveness. For example, operational testing could identify likely shot lines, hit points, burst points, or miss distances that might provide a context for LFT&E lethality assessments. Fuze performance, as determined under Developmental Test and Evaluation, could provide information for both Operational Test and Evaluation and LFT&E assessments.

9.4.5. Evaluation of Operational Suitability

Operational suitability is the degree to which a system can be satisfactorily placed in field use, with consideration given to reliability, availability, compatibility, transportability, interoperability, wartime usage rates, maintainability, safety, human factors, manpower supportability, logistics supportability, documentation, environmental effects, and training requirements.

Early planning for the suitability evaluation should include any special needs for number of operating hours, environmental testing, maintenance demonstrations, testing profiles, usability of Developmental Test data, or other unique test requirements.

Operational suitability should be evaluated in a mission context in order to provide meaningful results. For example, maintaining a required operations tempo over an extended period while conducting realistic missions gives insight into the interactions of various suitability factors.

9.4.6. Evaluation of Survivability

Survivability includes the elements of susceptibility, vulnerability, and recoverability. As such, survivability is an important contributor to operational effectiveness and suitability. A survivability assessment should be conducted for all systems under Operational Test and Evaluation (OT&E) oversight that may be exposed to threat weapons in a combat environment or to combat-induced conditions that may degrade capabilities, whether or not the program is designated for Live Fire Test and Evaluation (LFT&E) oversight. For example, unmanned

vehicles are not required to undergo survivability LFT&E under 10 USC 2366, but should be assessed for survivability. The assessment may identify issues to be addressed by testing.

The Developmental Test and Evaluation (DT&E), OT&E, and LFT&E strategies should be integrated so that the full spectrum of system survivability is assessed in a consistent manner. The Critical Operational Issues (COIs) should include the issues to be addressed in the OT&E evaluation of survivability. Personnel survivability must be addressed for systems under LFT&E oversight (reference 10 USC 2366) and should be integrated into the overall system evaluation of survivability conducted under OT&E.

Generally, vulnerability is addressed through LFT&E and susceptibility through OT&E, but there are areas of overlap. Realistic hit distributions are needed for the evaluation of LFT&E results. The OT&E evaluation of susceptibility might identify realistic hit distributions of likely threats, hit/burst points, and representative shot lines that might provide a context for LFT&E vulnerability assessments. Other LFT&E insights available from DT&E and OT&E testing of susceptibility might include information on signatures, employment of countermeasures, and tactics used for evasion of threat weapons. Similarly, LFT&E tests such as Total Ship Survivability trials might provide OT&E evaluators with demonstrations of operability and suitability in a combat environment.

Recoverability addresses the consequences of system damage. Typically, recoverability is primarily addressed by LFT&E. However, in general, tests relating to recoverability from combat damage or from peacetime accidents, battle damage assessment and repair, crashworthiness, crew escape, and rescue capabilities are of interest to both LFT&E and OT&E.

Real Time Casualty Assessment (RTCA) conducted during Initial Operational Test and Evaluation should be coordinated with LFT&E to ensure that assumptions supporting the RTCA are consistent with LFT&E results.

9.5. Live Fire Test and Evaluation (LFT&E)

9.5.1. Objective

The objective of Live Fire Test and Evaluation (LFT&E) is to provide a timely assessment of the vulnerability/lethality of a system as it progresses through its design and development prior to full-rate production. In particular, LFT&E should accomplish the following:

- Provide information to decision-makers on potential user casualties, vulnerabilities, and lethality, taking into equal consideration susceptibility to attack and combat performance of the system;
- Ensure that knowledge of user casualties and system vulnerabilities or lethality is based on testing of the system under realistic combat conditions;
- Allow any design deficiency identified by the testing and evaluation to be corrected in design or employment before proceeding beyond low-rate initial production; and
- Assess recoverability from battle damage and battle damage repair capabilities and issues.

The LFT&E Strategy for a given system should be structured and scheduled so that any design changes resulting from the testing and analysis, described in the LFT&E Strategy, may be incorporated before proceeding beyond low-rate initial production.

9.5.2. Covered Systems

"Covered system" is the DoD term that is intended to include all categories of systems or programs requiring Live Fire Test and Evaluation (LFT&E). A "covered system" means a system that Director, Operational Test and Evaluation, acting for the Secretary of Defense, has designated for LFT&E oversight. These include, but are not limited to, the following categories:

- Any major system within the meaning of that term in 10 USC 2302(5) that is user-occupied and designed to provide some degree of protection to its occupants in combat; or
- A conventional munitions program or missile program; or o a conventional munitions program for which more than 1,000,000 rounds are planned to be acquired (regardless of whether or not it is a major system); or
- A modification to a covered system that is likely to affect significantly the survivability or lethality of such a system.

9.5.3. Early Live Fire Test and Evaluation (LFT&E)

Director, Operational Test and Evaluation approves the adequacy of the LFT&E Strategy before the program begins LFT&E. The program should be driven by LFT&E issues identified in the strategy, and be fully integrated with planned Developmental Test and Evaluation and Operational Test and Evaluation. LFT&E typically includes testing at the component, subassembly, and subsystem level, and may also draw upon design analyses, modeling and simulation, combat data, and related sources such as analyses of safety and mishap data. This is standard practice, regardless of whether the LFT&E program culminates with full-up, system-

level (FUSL) testing, or whether a waiver is obtained from FUSL testing. One of the purposes of conducting LFT&E early in the program life cycle is to allow time to correct any design deficiency demonstrated by the test and evaluation. Where appropriate, the program manager may correct the design or recommend adjusting the employment of the covered system before proceeding beyond Low-Rate Initial Production.

9.5.4. Full-Up, System-Level (FUSL) Testing and Waiver Process

The term, "full-up, system-level testing," is the testing that fully satisfies the statutory requirement for "realistic survivability testing" or "realistic lethality testing" as defined in 10 USC 2366. The criteria for FUSL testing differ somewhat depending on whether the testing is for survivability or lethality. The following is a description of FUSL testing:

> Vulnerability testing conducted using munitions likely to be encountered in combat on a complete system loaded or equipped with all the dangerous materials that normally would be on board in combat (including flammables and explosives), and with all critical subsystems operating that could make a difference in determining the test outcome; or
>
> Lethality testing of a production-representative munition or missile, for which the target is representative of the class of systems that includes the threat, and the target and test conditions are sufficiently realistic to demonstrate the lethal effects the weapon is designed to produce.

The statute requires an Live Fire Test and Evaluation (LFT&E) program to include FUSL testing unless a waiver is granted in accordance with procedures defined by the statute. A waiver package must be sent to the Congressional defense committees prior to Milestone B; or, in the case of a system or program initiated at Milestone B, as soon as practicable after Milestone B; or if initiated at Milestone C, as soon as practicable after Milestone C. Typically, this should occur at the time of Test and Evaluation Master Plan (TEMP) approval.

The waiver package includes certification by the Under Secretary of Defense for Acquisition, Technology and Logistics or the DoD Component Acquisition Executive that FUSL testing would be unreasonably expensive and impractical. It also includes a Director, Operational Test and Evaluation (DOT&E)-approved alternative plan for conducting LFT&E in the absence of FUSL testing. Typically, the alternative plan is similar or identical to the LFT&E Strategy contained in the TEMP. This alternative plan should include LFT&E of components, subassemblies, or subsystems; and, as appropriate, additional design analyses, modeling and simulation, and combat data analyses.

Programs that have received a waiver from FUSL testing are conducted as LFT&E programs (with exception of the statutory requirement for FUSL testing). In particular, the TEMP contains an LFT&E Strategy approved by DOT&E, and DOT&E, as delegated by the Secretary of

Defense, submits an independent assessment report on the completed LFT&E to the Congressional committees as required by statute.

9.5.5. Personnel Survivability

Live Fire Test and Evaluation (LFT&E) has a statutory requirement to emphasize personnel survivability for covered systems occupied by U.S. personnel (10 USC 2366). In general, personnel survivability should be addressed through dedicated measures of evaluation, such as "expected casualties." The ability of personnel to survive should be addressed even in cases where the platform cannot survive. If the system or program has been designated by Director, Operational Test and Evaluation (DOT&E) for survivability LFT&E oversight, the program manager should integrate the test and evaluation to address crew survivability issues into the LFT&E program supporting the DOT&E LFT&E Report to Congress.

9.6. T&E Planning Documentation

9.6.1. Test and Evaluation Strategy (TES)

9.6.2. Test and Evaluation Master Plan (TEMP)

9.6.1. Test and Evaluation Strategy (TES)

9.6.1.1. Description

9.6.1.2. Content and Format

9.6.1.3. TES Approval Process

9.6.1.1. Description

The Test and Evaluation Strategy (TES) describes the concept for tests and evaluations throughout the program life cycle, starting with Technology Development and continuing through Engineering and Manufacturing Development (EMD) into Production and Deployment. The TES is submitted to OSD for approval prior to Milestone A/Key Decision Point A. The TES will evolve into the Test and Evaluation Master Plan (TEMP) at Milestone B/Key Decision Point B. Development of a TES will require early involvement of testers, evaluators, and others as a program conducts pre-system acquisition activities. These personnel will provide the necessary technical, operational, and programmatic expertise to ensure nothing is overlooked in laying out a complete strategy.

The TES must be consistent with the Technology Development Strategy and Initial Capabilities Document. The TES should address the identification and management of technology risk, the evaluation of system design concepts against the preliminary mission and sustainment

requirements resulting from the analysis of alternatives, competitive prototyping, early demonstration of technologies in relevant environments, and the development of an integrated test approach. The TES also satisfies the statutory requirement for a TDS test plan to ensure that the goals and exit criteria for the technology demonstrations are met (Section 235 of P.L. 107-314). It also provides a road map for evaluations, integrated test plans, and resource requirements necessary to accomplish the Technology Development phase objectives.

The TES begins by focusing on Technology Development phase activities, and describes how the component technologies being developed will be demonstrated in a relevant environment to support the program's transition into the EMD Phase. It contains hardware and software maturity success criteria used to assess key technology maturity for entry into EMD. For programs following an evolutionary acquisition strategy with more than one developmental increment, the TES should describe how test and evaluation (T&E) and modeling and simulation would be applied to each planned increment to provide the required operational effectiveness, suitability, and survivability, as would be required of a program containing only one increment. A TES is developed to support the initial Milestone A/Key Decision Point A decision and is replaced by the TEMP for all increments thereafter, unless a follow-on increment requires a new Milestone A decision. TES development establishes an early consensus among T&E Working-level Integrated Product Team member organizations on the scope of how the program will be tested and evaluated, with particular consideration given to needed resources, in order to support Planning, Programming, Budgeting, and Execution process activities. Cost estimates that need to be included in the TES should begin with program initiation through development and production, including nonrecurring and recurring research and development (R&D) costs for prototypes, engineering development equipment and/or test hardware (and major components thereof). Contractor T&E and Government support to the test program should be fully identified and estimated. Support, such as support equipment, training, data, and military construction should be estimated. The cost of all related R&D (such as redesign and test efforts necessary to install equipment or software into existing platforms) should be included. See DoD 5000.4-M, "Cost Analysis Guidance Procedures," Table C2.T2, "Defense Acquisition Program Life-Cycle Cost Categories Research and Development," for a more specific list of R&D costs. This cost information from the TES will be used as the basis for the T&E resources required for the Cost Analysis Requirements Description.

9.6.1.2. Content and Format

The following content and format is suggested for a Test and Evaluation Strategy (TES) to ensure that all necessary information is provided, and to assist in the transition to a Test and Evaluation Master Plan (TEMP) at Milestone B/Key Decision Point B.

PART I – INTRODUCTION

1.1. Purpose. State the purpose of the TES. Reference the documentation initiating the TES (i.e., Initial Capabilities Document (ICD), Analysis of Alternatives (AoA), Concept of Operations (CONOPS)).

1.2. Mission Description. Briefly summarize the mission need described in the capability requirements documents in terms of the capability it will provide to the Joint Forces Commander. Briefly summarize the CONOPS, and include an OV-1 or similar diagram.

1.3. System Description. Describe the system or prototype configurations. Identify key features, technologies, and components, both hardware and software for the planned Technology Development phase.

1.3.1. System Threat Assessment. Succinctly summarize the threat environment in which the system or components will operate. Reference the appropriate Defense Intelligence Agency- or DoD Component-validated threat documents.

1.3.2. Program Background. Briefly discuss any background information. Reference the AoA, the materiel development decision, and any previous tests or evaluations that have an effect on the test and evaluation (T&E) strategy.

1.3.3. Key Capabilities. Identify the system attributes that support key capabilities from the ICD. Identify the T&E-related TD Phase exit criteria.

1.3.3.1. Key Interfaces. Identify interfaces with existing or planned systems' architectures (to the extent known at Milestone A) that are required for mission accomplishment.

1.3.3.2. Special Test Requirements. Identify unique system characteristics or support concepts that will necessitate development of special test and evaluation assets or techniques.

1.3.3.3. Systems Engineering (SE) Requirements. Summarize SE-based information driving the Technology Development phase and prototype development. Reference the Systems Engineering Plan (SEP) and other applicable source documents.

PART II – TEST and EVALUATION PROGRAM MANAGEMENT AND SCHEDULE

2.1. T&E Management. Discuss the test and evaluation role of participating organizations. Describe the role of contractor and governmental personnel. Provide organizational construct that includes organizations such as the T&E Working-level Integrated Product Team or Service equivalent.

2.2. T&E Data Strategy. Describe the strategy and methods for collecting, validating, and sharing data as it becomes available from the contractors, Developmental Test and Evaluation (DT&E), and oversight organizations.

2.3. Integrated Test Program Schedule. Provide the overall time sequencing of the major events with an emphasis on the Technology Development phase. Include event dates such as major decision points, preliminary design reviews, prototypes and test article availability, and phases of DT&E.

PART III – TEST AND EVALUATION STRATEGY

3.1. T&E Strategy Introduction. This section should summarize an effective and efficient approach to the T&E program.

3.2. Evaluation Framework. Describe the overall concept of the T&E program with an emphasis on decisions in the Technology Development phase and information required to draft the Capability Development Document (CDD). Specific areas of evaluation should include Technology Readiness Level (TRL) and prototype testing. Include a Top-Level Evaluation Framework matrix that shows the correlation between decisions, the primary capabilities, critical technologies, critical technical parameters, and other key test measures.

3.3. Developmental Evaluation Approach. The discussion should be related to the Technology Development phase, including a focus on ICD issues. If applicable, discuss the T&E supporting the reliability growth approach.

3.3.1. Developmental Test Objectives. Summarize the planned objectives and state the methodology to test the technology attributes defined by the Technology Development Strategy (TDS).

3.3.2. Modeling & Simulation (M&S). Describe the key models and simulations and their intended use. Identify who will perform M&S verification, validation, and accreditation.

3.3.3. Test Limitations. Discuss any test limitations that may significantly affect the evaluator's ability to draw conclusions about the TRL and capabilities.

3.4. Operational Evaluation Approach. Discuss the approach during the Technology Development phase to providing operational insights from the user perspective, including resolution of the ICD issues. Include reliability growth testing, if appropriate.

3.4.1. Mission-Oriented Approach. Describe the approach to evaluate the system performance at the appropriate TRLs.

3.4.2. Operational Test Objectives. Summarize the planned objectives and state the methodology to test the technology attributes defined by the TDS.

3.4.3. M&S. Describe the key models and simulations and their intended use. Identify who will perform M&S verification, validation, and accreditation.

3.4.4. Test Limitations. Discuss any test limitations that may significantly affect the evaluator's ability to draw conclusions about the TRL and capabilities.

3.5. Future Test and Evaluation. Summarize all remaining significant T&E that has not been discussed yet, extending through the acquisition life cycle. Test events after Milestone B will be described in detail in the Milestone B TEMP update.

PART IV – RESOURCE SUMMARY

4.1. Introduction. Testing will be planned and conducted to take full advantage of existing DoD investment in ranges, facilities, and other resources wherever practical. Describe all key test and evaluation resources, both government and contractor, that will be used during the course of the Technology Development phase. Include long-lead items for the next phase, if known.

4.1.1. Test Articles. Identify the prototypes and test articles.

4.1.2. Test Sites and Instrumentation. Identify the test ranges and facilities to be used for testing.

4.1.3. Test Support Equipment. Identify test support, analysis equipment, and personnel required to conduct testing.

4.1.4. Threat Representation. Identify the type, number, availability, fidelity requirements, and schedule for representations of the threat (to include threat targets) to be used in testing.

4.1.5. Test Targets and Expendables. Specify the type, number, availability, and schedule for test targets and expendables, (e.g. targets, weapons, flares, chaff, sonobuoys, countermeasures).

4.1.6. Operational Force Test Support. Specify the type and timing of aircraft flying hours, ship steaming days, and on-orbit satellite contacts/coverage, and other operational force support.

4.1.7. Simulations, Models and Testbeds. Specify the models and simulations to be used. Identify opportunities to simulate any of the required support. Identify the resources required to validate and accredit their usage, responsible agency, and timeframe.

4.1.8. Joint Mission Environment. Describe the live, virtual, or constructive components or assets necessary to create an acceptable environment to evaluate TRLs and mission capabilities.

4.1.9. Special Requirements. Identify requirements for non-instrumentation capabilities or instrumentation and analysis tools that require development or upgrades.

4.2. Test and Evaluation Funding Summary. Provide initial estimates of DT&E, OT&E, and Live Fire Test and Evaluation costs.

9.6.1.3. Test and Evaluation Strategy (TES) Approval Process

For programs under OSD test and evaluation (T&E) oversight, the Program Manager or leader of the concept development team, with the T&E Working-level Integrated Product Team providing support, submits the DoD Component-approved TES to OSD for staffing and approval before Milestone A. The TES should be submitted at least 45 days prior to Milestone A to support the decision. The Director, Operational Test and Evaluation and Under Secretary of Defense for Acquisition, Technology and Logistics approve the TES for all programs on the OSD T&E Oversight List. For programs not on the OSD T&E Oversight List, the Component Acquisition Executive, or designated representative, approves the TES.

9.6.2. Test and Evaluation Master Plan (TEMP)

9.6.2.1. Description

All Major Defense Acquisition Programs, or programs on the OSD Test and Evaluation (T&E) Oversight List, are required to submit for OSD approval a Test and Evaluation Master Plan (TEMP) that describes the total T&E planning from component development through operational T&E into production and acceptance. The Program Manager (PM), with T&E Working-level Integrated Product Team (T&E WIPT) providing support, is responsible for producing the TEMP. It is an important document that identifies the required type and amount of test and evaluation events, along with their resource requirements. The TEMP is considered a contract among the PM, OSD, and the T&E activities. The PM must follow the approved TEMP to budget for T&E resources and schedules, which is why it is imperative that all T&E stakeholders participate early in the T&E strategy development and make timely updates when events or resource requirements change. Stakeholders should include representatives from Under Secretary of Defense for Acquisition, Technology and Logistics and Director, Operational Test and Evaluation (DOT&E), as those offices ultimately will approve the TEMP. Their representatives can advise on what would constitute acceptable Developmental Test and Evaluation, Operational Test and Evaluation, and, if appropriate, Live Fire risk reduction strategies, and can ensure programs are satisfying statutory and regulatory T&E requirements.

While the program manager is responsible for developing the TEMP, the T&E WIPT should make every effort to complete the TEMP in a timely manner and resolve any outstanding issues.

Each WIPT member should make every attempt to ensure its organization's issues are surfaced during WIPT meetings to avoid surprises during staffing. If the T&E WIPT cannot resolve all the issues in a timely manner, the program manager should raise the issues for resolution via the Integrated Product and Process Development process.

The TEMP focuses on the overall structure, major elements, and objectives of the T&E program and must be consistent with the Technology Development Strategy, Acquisition Strategy, approved Capability Development Document (CDD) or Capability Production Document (CPD), System Threat Assessment, and Information Support Plan. The TEMP should be consistent with and complementary to the Systems Engineering Plan. For a program using an evolutionary acquisition strategy, the TEMP must also be consistent with the time-phased statement of desired capabilities in the CDD or CPD. It provides a road map for evaluations, integrated test plans, and resource requirements necessary to accomplish the T&E program objectives. The TEMP must also be consistent with the DOT&E's intended schedule for complying with the statutory reporting requirements for Operational Test and Evaluation and/or Live Fire Test and Evaluation (LFT&E), whether through the phased submittal of dedicated reports or on the Beyond-Low-Rate Initial Production or LFT&E reports, or through DOT&E's Annual Report to the Congress.

9.6.2.2. Evaluation Framework

A test and evaluation (T&E) program strategy should be structured to provide knowledge to reduce risk in acquisition and operational decisions. That knowledge is developed through the evaluations of all available and relevant data and information from contractor and government sources. The evaluation framework describes the links between key program and user decisions, and the operational and developmental areas that must be evaluated for those decisions. It correlates the knowledge required concerning key performance parameters (KPPs)/key system attributes (KSAs), critical technical parameters (CTPs), key test measures (i.e., measures of effectiveness (MOEs) and measures of suitability (MOSs)), and the planned test methods, key test resources, facility, or infrastructure needs. The framework discussion should also identify major risks or limitations to completing the evaluations. The Test and Evaluation Master Plan (TEMP) reader should be left with a clear understanding of what key questions evaluations will answer for the program and user, and at what key decision points. This layout and discussion will also provide rationale for the major test objectives and the resulting major resource requirements shown in the TEMP Part IV – Resources.

Within the evaluation framework there should be discussions of the intended maturation of key technologies and the overall system, the evaluation of capabilities in a mission context, and evaluations needed to support required certifications or to comply with statute. The details of how the evaluations will be performed should be left to separate evaluation plans (e.g., System Evaluation Plan (Army), Operational Test and Evaluation plan, Live Fire Test and Evaluation plan).

The evaluation of the maturation of a system or capability is described in the Developmental Test and Evaluation section, and should address the overall approach to evaluate development of

system capabilities. The approach should cover critical technical parameters, key system risks, and any certifications required (weapon safety, interoperability). The evaluation of technology maturity should support the Technology Development Strategy. The evaluation of system maturity should support the acquisition strategy. The extent of this discussion will be driven by the amount of development in the acquisition strategy. For example, if the system is a non-developmental item (i.e., Commercial-off-the-shelf (COTS) or Government-off-the-shelf) then there may not be much, if any, maturation of the system required. If the system is a new technologies effort, pushing the state-of-the-art or capabilities significantly improved over what is currently being achieved in the operational environment, then there may be a significant amount of effort in maturing or developing the system or its support system, and therefore more decisions requiring knowledge from evaluations. In assessing the level of evaluations necessary, equal consideration should be given to the maturity of the technologies used, the degree to which system design (hardware and software) has stabilized, as well as the operational environment for the employment of the system. A lesson learned from prior programs, is that using a COTS item in a new environment can result in a significant change in capability, and therefore is not really a COTS item from a system maturity perspective.

The system maturation discussions should also cover evaluations for production qualification, production acceptance, and sustainment of the system. The production evaluations may be covered by Defense Contract Management Agency (DCMA) representatives and procedures at the contractors manufacturing plant, or they may require T&E effort to establish and mature the processes. Therefore, the appropriate level of evaluation could range from none, for normal DCMA practices, to minimal for first article qualification checks, to more extensive evaluations based upon production qualification test results for new or unique manufacturing techniques, especially with new technologies. The sustainment evaluation discussions should address the key risks or issues in sustaining or assessing the system capability in operational use. The sustainment evaluation discussion should address the overall logistics T&E effort, maintenance (both corrective and preventative), servicing, calibration, and support aspects.

The discussion of mission context evaluations addresses the approach to evaluate operational effectiveness and operational suitability of the system for use by typical users in the intended mission environments. This should also include joint operations issues. These evaluations provide a prediction of how well the system will perform in field use and in the Initial Operational Test and Evaluation (IOT&E) and may be used to reduce the scope of the IOT&E, but shall not replace or eliminate the need for IOT&E.

Include in this discussion the critical operational issues (COIs). COIs are the operational effectiveness and operational suitability issues (not parameters, objectives, or thresholds) that must be examined to evaluate/assess the system's capability to perform its mission. Not all operational issues are critical – COIs must be relevant to the required capabilities, of key importance to the system being operationally effective and suitable, and represent a significant risk if not satisfactorily resolved.

The evaluation strategy must include those evaluations required by statute, specifically IOT&E, survivability, and lethality. The IOT&E discussion should describe the approach to conduct the independent evaluation of the system, including official resolution of the COIs. The discussion of the approach to evaluate the survivability/lethality of the system should show how it will influence the development and maturation of the system design. The discussion should include a description of the overall live fire evaluation strategy for the system (as defined in 10 USC 2366); critical live fire evaluation issues; and any major evaluation limitations.

The evaluation framework discussions should concisely articulate links between key decisions in the system life cycle, the areas that need to be evaluated to support those decisions, and an outline of the test methodologies needed to obtain the data for the evaluations. The evaluation framework discussions should be supplemented with a table or matrix that provides a concise visual summation of the framework discussions. Figure 3.1, "Top-Level Evaluation Framework Matrix," in the sample TEMP format section shows one way an evaluation framework table or matrix can be organized. Equivalent Service-specific formats that identify the same relationships and information are appropriate. The matrix in the TEMP is an executive level view that should provide building blocks for more detailed matrixes and links within supporting test plans.

The evaluation matrix is divided into three sections–Decisions Supported; Key Requirements and T&E Measures; and Test Methodologies/Key Resources.

Decisions Supported – These are the major design, developmental, manufacturing, programmatic, acquisition, or employment decisions driving the need for knowledge to be obtained through T&E. These decisions include acquisition milestones/key decision points, design reviews, certifications, safety releases, production acceptance, and operational employment/deployment. The operational employment/deployment decisions include those made by operators and maintainers that drive the need for validated operating and maintenance manuals. The decisions supported column would not contain each decision that an operator or maintainer would make, but just the overall level of knowledge needed for operating or maintenance data or instructions, or those that steer significant or top-level decisions. The key determinant on what to include in this section is whether the decision supported (or knowledge requirement) drives trade space for performance, cost or schedule, or the size or scope of the T&E program. Only those decisions that facilitate program decisions or the size or scope of the T&E program should be included.

Key Requirements and T&E Measures – These are the KPPs and KSAs and the top-level T&E issues and measures for evaluation. The top-level T&E issues would typically include COIs and COI Criteria (COIC), CTPs, and key MOEs/MOSs. System-of-systems issues should also be included. Each measure should be associated with one or more key requirements. However, there could be T&E measures without an associated key requirement or COI/COIC. Hence, some cells in Figure 3.1 may be empty. A simple test to determine if this section of the matrix is minimally adequate is to confirm that each decision supported has at least one T&E measure associated with it, and that each key requirement also has at least one T&E measure associated with it.

Outside of that, only include the T&E issues and measures that drive size or scope of the T&E program.

Overview of Test Methodologies and Key Resources – These identify test methodologies or key resources necessary to generate data for evaluations to support decisions. The content of this column should indicate the key methodologies or significant resources that will be required. Test methodology refers to high-level descriptions of methods used to obtain the data. For example, modeling and simulation, system integration lab, or open-air range, each represent a different methodology for obtaining test data. Where multiple methodologies are acceptable, show the preferred methodology that will be used. Short notes or acronyms should be used to identify the methodology. Models or simulations should be identified with the specific name or acronym.

9.6.2.3. Approval Process

The Test and Evaluation Master Plan (TEMP) for an OSD Test and Evaluation (T&E) Oversight program is submitted by the DoD Component to the TEMP approval authorities. The Director, Operational Test and Evaluation (DOT&E) and the Director, Developmental Test and Evaluation (DDT&E) approve the TEMP for all programs on the OSD T&E Oversight List. For other programs, the Component Acquisition Executive (CAE), or designated representative, approves the TEMP.

For OSD T&E oversight programs, the Office of the Director, DT&E staffs the document through appropriate OSD organizations for coordination, formally concurs on the adequacy of the TEMP, approves the TEMP for the USD(AT&L), and then forwards it to DOT&E. For programs not on the OSD T&E oversight list, the document is submitted to the CAE for approval.

A TEMP must be submitted not later than 45 days prior to the Milestone/Key decision point or subsequent program initiation if a Program Manager must have an OSD-approved document by the decision date. For programs newly added to the OSD T&E Oversight List, the TEMP must be submitted within 180 days of such written designation.

9.6.2.4. Test and Evaluation Master Plan (TEMP) Updates

TEMPs are first required at milestone/key decision point entry into the acquisition life cycle. TEMPs are required to be updated at Milestone C and the Full Rate Production Decision Review, but should also be updated when the program baseline has been breached, when the associated Joint Capabilities Integration and Development System document or Information Support Plan has been significantly modified, or on other occasions when the program is significantly changed or restructured. Evolutionary acquisition programs may require additional updates to ensure that the TEMP reflects the currently defined program. When a program baseline breach occurs, the TEMP should be updated within 120 days of the date of the Program Manager's (PM's) Program Deviation Report to ensure it reflects the restructured program. When a program changes

significantly, the TEMP due date will be negotiated between the PM and the DoD Component TEMP approval authority. In the case of programs under OSD T&E oversight, the negotiations will take place between the PM, DoD Component TEMP approval authority, USD(AT&L), and DOT&E. In either case, the goal should be to update the TEMP within 120 days.

9.6.2.5. Circumstances When a Test and Evaluation Master Plan (TEMP) is No Longer Required

When a program's development is completed and Critical Operational Issues are satisfactorily resolved, including the verification of deficiency corrections, TEMP updates are no longer required. The following attributes are examples for which an updated TEMP submission may no longer be required:

- Fully deployed system with no operationally significant product improvements or increment modification efforts;
- Full production ongoing and fielding initiated with no significant deficiencies observed in production qualification test results;
- Partially fielded system in early production phase having successfully accomplished all developmental and operational test objectives;
- Programs for which planned test and evaluation is only a part of routine aging and surveillance testing, service life monitoring, or tactics development;
- Programs for which no further operational testing or live fire testing is required by any DoD Component; and/or
- Program for which future testing (e.g., product improvements or incremental upgrades) has been incorporated in a separate TEMP (e.g., an upgrade TEMP).

9.6.2.6. Requesting Cancellation of Test and Evaluation Master Plan (TEMP) Requirement

Written requests for cancellation of a TEMP requirement for a program under OSD test and evaluation oversight must be forwarded through the DoD Component TEMP approval authority to the office of the Director, Developmental Test and Evaluation. Justification, such as applicability of any the above circumstances, must be included in the request. The Director, Developmental Test and Evaluation will jointly review the request with Director, Operational Test and Evaluation and notify the DoD Component TEMP approval authority of the result.

9.7. Test and Evaluation (T&E) Reporting of Results

9.7.1. DoD Component Reporting of Test and Evaluation (T&E) Results

9.7.2. Developmental Test and Evaluation (DT&E) Final Report

9.7.3. Live Fire Test and Evaluation (LFT&E) Report

9.7.4. Beyond Low-rate Initial Production (LRIP) Report

9.7.5. Director, Operational Test and Evaluation (DOT&E) Annual Report

9.7.1. DoD Component Reporting of Test and Evaluation (T&E) Results

DoD Instruction 5000.02 requires the Program Manager of a program designated for OSD T&E oversight to provide reports of results, conclusions, and recommendations from Developmental Test and Evaluation (DT&E), Operational Test and Evaluation, and Live Fire Test and Evaluation to Director, Operational Test and Evaluation and Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) (or as delegated/designated). For those reports supporting a decision point, the report should be submitted 45 days before the decision point. In addition, program managers will report the results of completed developmental testing to the milestone decision authority at Milestones/key decision points B and C. The report will identify the strengths and weaknesses in meeting the warfighters documented needs based on developmental evaluations. Although the program manager has the responsibility to report the DT&E results, the program manager has the option to have the DT&E Responsible Test Organization (RTO) provide the briefing of results. Regardless of who actually briefs the results, the content of the report is the impartial evaluation from the DT&E RTO of a system's military utility and capabilities against warfighter requirements.

All developmental and operational T&E agencies will identify test and evaluation limitations. Their assessment should include the effects of these limitations on evaluations of system performance, and on the ability to assess performance or operational capabilities.

9.7.2. Developmental Test and Evaluation (DT&E) Final Report

For each program on the OSD T&E Oversight list, the DT&E Responsible Test Organization (RTO) should prepare a written report at the completion of the DT&E described in the Test and Evaluation Master Plan (TEMP). The DT&E report will provide a historical record of the final test and evaluation results for the system. In addition, the report should include the RTO's assessment of a system's military utility, capabilities and limitations; document the test techniques, procedures, and data analysis concepts; and provide data for operating/employment and maintenance manuals for the system. DT&E final reports should be submitted to the Defense Technical Information Center (DTIC) for inclusion in their repository.

9.7.3. Live Fire Test and Evaluation (LFT&E) Report

Director, Operational Test and Evaluation (DOT&E) monitors and reviews the LFT&E of each covered system. At the conclusion of LFT&E, the Director prepares an independent assessment report that:

- Describes the results of the survivability or lethality LFT&E, and
- Assesses whether the LFT&E was adequate to provide information to decision-makers on potential user casualties and system vulnerability or lethality when the system is employed in combat, and to ensure that knowledge of user casualties and system vulnerabilities or lethality is based on realistic testing, consideration of the validated statement of desired operational capabilities, the expected threat, and susceptibility to attack.

DOT&E prepares the OSD LFT&E Report within 45 days after receiving the DoD Component LFT&E Report, which is required by DoD Instruction 5000.02. The Secretary of Defense (or DOT&E if so delegated) submits the OSD LFT&E report to Congress before a covered system proceeds beyond Low-Rate Initial Production (LRIP) (10 USC 2366). If the system is designated for both Operational Test and Evaluation (OT&E) and LFT&E oversight, DOT&E may choose to combine the LFT&E and Beyond LRIP Reports under single cover, so as to better integrate the reporting of LFT&E and OT&E.

9.7.4. Beyond Low-rate Initial Production (LRIP) Report

To meet the statutory requirements of 10 USC 2399, Director, Operational Test and Evaluation (DOT&E) analyzes the results of IOT&E conducted for each MDAP program. At the conclusion of Initial Operational Test and Evaluation (IOT&E), the Director prepares a report stating the opinion of the Director as to:

- Whether the test and evaluation (T&E) performed were adequate; and
- Whether the results of such T&E confirm that the items or components actually tested are effective and suitable for combat, and
- Additional information on the operational capabilities of the items or components that the Director considers appropriate based on the testing conducted.

The Director submits Beyond-LRIP Reports to the Secretary of Defense, Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)), and the congressional defense committees. Each such report is submitted to those committees in precisely the same form and with precisely the same content as the report originally was submitted to the Secretary and USD(AT&L) and shall be accompanied by such comments as the Secretary may wish to make on the report. A final decision within the Department of Defense to proceed with an Major Defense Acquisition Program (MDAP) beyond LRIP may not be made until the Director has submitted to the Secretary of Defense the Beyond-LRIP Report with respect to that program and the congressional defense committees have received that report.

If a decision is made to proceed to operational use before a final decision is made for a MDAP to proceed beyond LRIP, DOT&E will submit to the Secretary of Defense and the congressional defense committees, a Beyond-LRIP Report with respect to that program as soon as practicable.

If the report indicates that either Operational Test and Evaluation was not adequate or that the system as tested was not effective or not suitable, DOT&E will continue to report his or her assessment of test adequacy and system operational effectiveness and suitability, based on Follow-on Operational Test and Evaluation, in the DOT&E Annual Report (see below).

In evolutionary acquisition programs that conduct a separate IOT&E for successive development configurations or increments, DOT&E may submit separate Beyond LRIP Reports, or if the scope of the configuration change is minimal, may use the DOT&E Annual Report for the purpose of notifying Congress and the Secretary.

9.7.5. Director, Operational Test and Evaluation (DOT&E) Annual Report

DOT&E prepares an annual Operational Test and Evaluation (OT&E) and Live Fire Test and Evaluation (LFT&E) report, in both classified and unclassified form, summarizing all OT&E and LFT&E activities, and addressing the adequacy of test resources within the Department of Defense during the previous fiscal year (10 USC 139). The report includes the status of information assurance, Electromagnetic Environmental Effects, and interoperability for each program. The report also includes an assessment of the waivers of and deviations from requirements in test and evaluation master plans and other testing requirements that occurred during the fiscal year, any concerns raised by the waivers or deviations, and the actions that have been taken or are planned to be taken to address the concerns (Pub.L. 107-314, Sec. 235). DOT&E submits the reports concurrently to the Secretary of Defense, Under Secretary of Defense for Acquisition, Technology and Logistics, and Congress, within 10 days of the President's Budget to Congress.

9.8. Best Practices

9.8.1. Developmental Test and Evaluation (DT&E) Best Practices

DT&E "best practices" vary widely in scope and applicability to other programs. Lessons learned or relearned in other test and evaluation (T&E) programs present an opportunity for future programs to avoid issues, enhance their T&E effectiveness and efficiency, and enable better decisions with limited T&E time/resources.

9.8.2. OT&E Best Practices

Learn something each year

Use a phased approach that identifies key decision points and that generates timely and objective information for decision makers on the system's demonstrated capabilities to date (i.e., learn something each year).

Focus on the mission(s)

Focus on the mission(s) a unit or crew equipped with this system is expected to accomplish. Identify the operational capabilities that will be critical to mission accomplishment. (This starts a "top-down" methodology leading to critical operational issues (COIs), measures of effectiveness (MOEs), critical Live Fire Test and Evaluation (LFT&E) issues, and other evaluation issues, measures of performance, and data requirements. These are ultimately to be "rolled back up" to assess the degree of mission accomplishment. The resulting Operational Test and Evaluation (OT&E) concept will link mission accomplishment to the key operational capabilities that are identified in the Joint Capabilities Integration and Development System documents as the basis for accepting the system.)

Consider the employment of the system

During planning, consider how the system will be employed and sustained to accomplish the mission(s) previously described. Describe the steps of a complete mission cycle, from mission tasking through successful execution and return, followed by the actions required for the system to be able to perform another mission cycle. Consider organizational structure; tactics, techniques, and procedures; training; and any required supporting systems. This provides a "system-of-system" perspective that gives insight into any important interoperability requirements. Determining the appropriate external systems, measures, operational context, and mix of live virtual and constructive resources will depend on the particular system and situation.

Each increment must be militarily useful and supportable

For programs using evolutionary acquisition, the ultimate functionality may or may not be defined at the beginning of the program. Each increment, however, must provide a militarily useful and supportable operational capability, with thresholds and objectives set by the user. The Test and Evaluation Strategy should provide for an evaluation of the ability of each increment to meet the user's thresholds and evaluate the potential for growth. Comparisons of the capabilities of the legacy system or baseline and the planned increment may assist in evolutionary acquisition by answering the question of whether the new increment provides enough of an improvement in mission capability to warrant fielding to the force.

Follow Director, Operational Test and Evaluation (DOT&E) guidelines for software systems

For software-intensive systems, follow the DOT&E Guidelines for Conducting Operational Test and Evaluation (OT&E) for Software-Intensive System Increments.

COIs should be few in number

During planning, the study of the mission, desired performance capabilities, employment concept, and studies such as analyses of alternatives, lead to a set of COIs and critical LFT&E issues whose satisfactory resolution is vital to the system's operational effectiveness, suitability, and survivability evaluation. The COIs should be few in number, operational in nature, observable, and testable. They should address mission accomplishment and survivability at a level (e.g., ship, flight, unit) appropriate to the evaluation required.

Provide a comparison to the baseline system

Whenever applicable, provide a measurable means for comparisons to a baseline system. Baseline comparisons can reduce risk to the program by demonstrating possible improvement in overall mission capability even if certain technical performance requirements are not met. Use of a baseline may reduce risks to test adequacy by compensating for unexpected problems with test environment, training of the test unit, or data collection. Finally, comparisons to the baseline system can demonstrate the degree to which the original deficiencies (in terms of mission accomplishment) have been corrected.

Look for opportunities to integrate testing

Identify proposed sources of data for the MOEs and measures of performance associated with each COI, LFT&E issue, and secondary evaluation issue. In addition to the Initial Operational Test and Evaluation (IOT&E), consider other operational events, as well as live fire tests, key developmental test events, modeling and simulation, dedicated side tests, excursions, and "piggy-back" on training or other planned testing opportunities. Look for opportunities to integrate LFT&E and OT&E.

Realistically stress systems during DT

Realistically stress systems during developmental testing. Do not let IOT&E be the first time that the system is exposed to operationally realistic environments.

Test in extreme environments

Test in extreme environments - chambers are necessary but not sufficient to understand system capabilities and limitations.

Involve the Operational Test Agencies (OTAs) and OSD early

Involve the OTAs, intelligence agencies, and OSD (for OSD oversight programs) early in the program design stages.

9.8.3. Live Fire Test and Evaluation (LFT&E) Best Practices

Pretest Predictions

Pretest predictions are standard practice for every live fire test event. The predictions may be based on computer models, engineering principles, or engineering judgment, and should address a level of detail comparable to the test damage assessment methodology. The Director, Operational Test and Evaluation-approved LFT&E Strategy should address both the nature of the pretest predictions and the schedule of pretest prediction deliverables. The deliverables and supporting documentation should identify basic assumptions, model inputs, and known limitations. If the live fire evaluation plan incorporates the use of vulnerability or lethality models, the pretest predictions should exercise those models, and support the verification, validation, and accreditation of those models. Adequate time and resources should be planned to support pre-test predictions and post-test reconciliation of models and test results.

Evaluation Measures

Although the evaluation of live fire test results will address kill given a hit (i.e., vulnerability or lethality), the outcome of LFT&E is not necessarily expressed in terms of probabilities. Rather, live fire testing typically addresses vulnerability or lethality primarily by examining basic damage and kill mechanisms and their interactions with the target system. Further, the evaluation of vulnerability test results should address, where possible, the susceptibility and recoverability of the system and be integrated with results of Operational Test and Evaluation.

9.9. Special Topics

9.9.1. Interoperability

For Information Technology (IT) systems, including National Security Systems (NSS), with interoperability requirements, the Joint Interoperability Test Command (JITC) is required to provide system Net-Ready certification memoranda to the Director, Joint Staff J-6, throughout the system life cycle and regardless of acquisition category. Based on net readiness evaluations and other pertinent factors, the Joint Staff J-6 shall issue Net-Ready System Certification memoranda to the respective DoD Components and developmental and operational test organizations in support of the Full-Rate Production (FRP) Decision Review.

Net readiness applies to Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems and to any weapon or system that share data. In general, every system is required to have a Net-Ready Key Performance Parameter (KPP) (NR-KPP) and be certified for net readiness. Net-Ready certification is required for a FRP decision, and acceptable net readiness must be demonstrated prior to a Milestone C Low-Rate Initial Production decision and Initial Operational Test and Evaluation (IOT&E). Final certification for NR-KPP is routinely assessed in conjunction with IOT&E, but documented separately through JITC and Joint Staff J-6. In addition, systems will be tested and evaluated periodically over their life cycle for net readiness.

As with most other aspects of a system, net readiness is an early consideration for design and test. The strategy for evaluating net readiness should be included in the Test and Evaluation Master Plan (TEMP). An important aspect is to develop a strategy for testing each system in the context of the system-of-systems, or family-of-systems architecture within which it is required to operate.

The JITC is DoD's test organization for net readiness. JITC is the agency that will facilitate a system's Net-Ready certification. The philosophy employed by JITC is to leverage other planned test events to generate necessary data for Net-Ready certification. A special test will be necessary only if other events do not provide the appropriate data. It is important that JITC be included as a member of the T&E Working-level Integrated Product Team, and participates in the TEMP development.

9.9.2. Evaluations for System Assurance

System assurance evaluations provide the program manager and systems engineer with knowledge to establish a level of confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle. System assurance activities are executed at every stage of the program's management and development life cycle. System assurance is a broad area, encompassing information assurance, anti-tamper, and other critical program information protection measures. Information assurance and anti-tamper are briefly discussed in the subsections below. For additional background and guidance on system assurance, see the following:

- Engineering for System Assurance
- DoD Instruction 5200.39, "Critical Program Information (CPI) Protection Within the Department of Defense"
- USAF Software Technology Support Center (STSC) CrossTalk article.

9.9.3. Critical Program Information (CPI) Countermeasure Components

In addition to the two components provided here, a comprehensive set of CPI Countermeasures is listed in Chapter 8.

9.9.3.1. Information Assurance (IA) Considerations

The test and evaluation (T&E) of IA requirements is an integral part of the overall T&E process. DoD Instruction 5000.02 directs that IA test and evaluation be conducted during both Developmental Test and Evaluation and Operational Test and Evaluation.

To ensure that IA testing adequately addresses system IA requirements, all sources of IA requirements must be considered. The primary source is the applicable set of baseline IA controls that are described in section 7.5.7.2 of this document. In addition, some capabilities documents (e.g., Initial Capabilities Document, Capability Development Document, and Capability Production Document) may specify IA requirements. Additional IA requirements may be identified as a result of the risk management process, or as directed by the DoD Components.

It is important to consider the impact of the DoD Information Assurance Certification and Accreditation Process (DIACAP) on the overall T&E schedule. An Interim Authorization to Operate or Authorization to Operate is required prior to conducting Operational Test. These authorizations are granted only after the bulk of Certification and Accreditation (C&A) activities are concluded, and the Designated Accrediting Authority is satisfied with the residual risk to the system. Significant C&A activities and events should be visible on the integrated test schedule to ensure appropriate coordination of events.

9.9.3.2. Testing for Anti-Tamper (AT)

The AT implementation is tested and verified during Developmental Test and Evaluation and Operational Test and Evaluation. The program manager develops the validation plan and provides the necessary funding for the AT verification and validation (V&V) on actual or representative system components. The V&V plan, which is developed to support Milestone C, is reviewed and approved by the AT Executive Agent, or any DoD Component-appointed AT Agent, prior to the milestone decision. The program office conducts the V&V of the implemented AT plan. The AT Executive Agent witnesses these activities and verifies that the AT plan is implemented into the system and works according to the AT plan. The program manager and the AT Executive Agent may negotiate for parts of the system that have undergone anti-tamper measures to be tested at the AT Executive Agent's laboratories for further analysis. The validation results are reported to the Milestone Decision Authority.

9.9.4. Electromagnetic Environment Effects (E3) Testing

E3 can adversely affect the operational effectiveness of military forces, equipment, systems, and platforms. Additionally, today's complex military operational environment is characterized by an increasingly congested electromagnetic spectrum coupled with a reduction of spectrum allocated for exclusive military use. The mix of DoD-developed and commercial-off-the-shelf electronic equipment increases the importance of effectively managing E3 and spectrum usage in the battle space. It is the responsibility of the program manager to ensure, and the responsibility of the Developmental and Operational Test Agencies to validate, the readiness of systems to be fielded into this environment. Historically, failure to verify equipment/platform electromagnetic compatibility in the item's intended operational electromagnetic environment have caused costly program delays and adversely affected operational safety, suitability, and effectiveness.

A series of evaluations should be conducted to demonstrate that an item's engineering design is complete and sound, that E3 have been effectively controlled and that E3 limitations and vulnerabilities have been identified and documented. These evaluations and the associated test requirements vary depending on the item under consideration and the operational Electromagnetic Effects associated with its intended use. General test requirements and guidelines for electromagnetic compatibility are contained in MIL-STD-461 (*login*, then URL: https://assist.daps.dla.mil/online/parms/mainframe.cfm?ident_number=35789). E3 requirements for systems can be found in MIL-STD-464 (*login*, then URL: https://assist.daps.dla.mil/online/parms/mainframe.cfm?ident_number=35794) and MIL-HDBK-237 (*login*, then URL: https://assist.daps.dla.mil/online/parms/mainframe.cfm?ident_number=53956). These evaluations should be initiated at the earliest practical point in the item's life cycle so that deficiencies can be identified early and corrected. Program managers are encouraged to contact their DoD Component E3 representatives to establish an E3 control and evaluation plan for their acquisition program.

9.9.4.1. Hazards of Electromagnetic Radiation to Ordnance (HERO)

In DoD terminology, the hazards that result from adverse interactions among radio frequency (RF) emitters and electrically initiated devices (EID) or initiating systems contained within ordnance systems (e.g., fuses) are referred to as HERO. Where applicable, HERO tests should be conducted to determine if exposure of electrically initiated ordnance to specified electromagnetic environment (EME) levels will adversely affect the ordnance. The general approach for HERO testing is to expose inert, instrumented ordnance to a controlled test EME and to monitor each EID contained within the ordnance for a possible response. For most EIDs, the response is quantified in terms of the magnitude of RF current induced into the heating element, or bridge wire, of the device. A common objective in all HERO testing is to determine the maximum or worst case response at various test frequencies for various ordnance physical configurations. HERO testing should emphasize exposure of the ordnance to the EME levels that are associated with each operational phase of an ordnance item to include assembly/disassembly, staged, handling and loading, platform loaded, immediate post launch, transportation and storage. Detailed guidance on HERO testing can be found in MIL-HDBK-240, (*login*, then URL: https://assist.daps.dla.mil/online/parms/mainframe.cfm?ident_number=212331) "HERO Test Guide."

9.9.4.2. Hazards of Electromagnetic Radiation to Personnel (HERP)

A potential hazard can exist when personnel are exposed to an electromagnetic field of sufficient intensity to heat the human body. The potential for electromagnetic radiation (EMR) to produce harmful biological effects in humans is referred to as HERP. Radar and electronic warfare systems present the greatest potential for personnel hazard due to their high transmitter output powers and antenna characteristics. Where applicable, HERP tests should be conducted to establish safety tolerance levels for exposure to EMR as defined in DoD Instruction 6055.11.

9.9.4.3. Hazards of Electromagnetic Radiation to Fuels (HERF)

An electromagnetic field of sufficient intensity can create sparks with sufficient energy to ignite volatile combustibles, such as fuel. The potential for electromagnetic radiation to cause ignition or detonation of volatile combustibles, such as fuels, is referred to as HERF. The existence and extent of a fuel hazard are determined by comparing the actual radio frequency power density to an established safety criterion. When applicable, HERF tests should be conducted to establish safe operating distances.

9.9.5. Support for Joint Munitions Effectiveness Manuals (JMEM)

Each DoD Component should provide weapons effectiveness data for weapons in the acquisition process to Director, Operational Test and Evaluation for use in the JMEM. The DoD Component should provide the data prior to the weapon achieving initial operational capability, and should prepare the data in coordination with the Joint Technical Coordinating Group for Munitions Effectiveness.

9.9.6. Spectrum Management Support

To evaluate spectrum availability, spectrum-related operational restrictions, frequency availability, host nation approvals, electromagnetic compatibility, and other such issues should be considered. A spectrum management operational test assessment is essentially a review of the spectrum management process for the system/equipment in question. Developmental Test and Evaluation and the early phases of Operational Test and Evaluation, if appropriate, should determine if spectrum management issues are resolved, prior to Developmental Performance Verification Testing (DPVT). All systems/equipment that have spectrum requirements normally undergo DPVT. The Component Acquisition Executive should review unresolved spectrum management issues when evaluating system readiness for Initial Operational Test and Evaluation.

9.9.7. Environment, Safety, and Occupational Health

The Test and Evaluation Master Plan (TEMP) should address the program manager's analysis of residual Environmental, Safety and Occupational Health (ESOH) risks and control measures, to include safety releases, for the system or item. The intent is to ensure that, prior to Operational Test and Evaluation and fielding, the testers and users understand the ESOH hazards, the control measures adopted by the program manager, and the residual risks accepted by the program manager. Early participation of ESOH expertise in system requirements development and on the Test and Evaluation Working-level Integrated Product Team is recommended to assure appropriate issues are addressed during test planning and execution.

The program manager, working with the range or facility commanders, must ensure compliance with National Environmental Policy Act (NEPA)/Executive Order (E.O.) 12114 requirements, particularly as they affect test ranges and operational areas. The TEMP should include NEPA/E.O.12114 documentation requirements, and describe how analyses will be conducted to support test site selection decisions.

DoD Instruction 5000.02, Enclosure 6, paragraph 1.b requires the Program Manager (PM) to provide safety releases to developmental and operational testers prior to any test using personnel. A Safety Release communicates to the activity or personnel performing the test the risks associated with system operation, and the mitigating factors required, ensuring safe operation of the system. A secondary function of the process is to ensure that due diligence is practiced with respect to safety in the preparation of the test. A Safety Release is normally provided by the PM after appropriate hazard analysis. Safe test planning includes analysis of the safety release, in addition to safety reviews of test procedures, equipment, and training. An interim safety release is usually provided prior to developmental testing, with a full safety release expected before Initial Operational Test and Evaluation.

9.9.8. Testing in a Joint Environment

The phrase *testing in a joint environment* originated in U.S. Department of Defense 2006-2011 Strategic Planning Guidance for Joint Testing in Force Transformation. It refers to testing military systems as participating elements in overarching joint systems-of-systems. This testing in a joint environment initiative is in support of the department's long-term strategy to test as we fight. Joint operations have become the mainstay of war fighting. Force transformation will require the Test and Evaluation (T&E) community to place a greater emphasis on testing joint war fighting capabilities developed in response to the Joint Capabilities Integration and Development System. Future T&E must make sure that combatant commanders can rely on equipment to operate together effectively without introducing problems to warfighters. For a detailed discussion of changes needed to bring about this vision of T&E, see the Testing in a Joint Environment Roadmap that was signed by the Deputy Secretary of Defense in November 2004. The proposals in this roadmap are important enablers for acquiring new systems that are *born joint* and testing legacy equipment and systems that are made joint.

The joint mission environment is defined as, "a subset of the joint operational environment composed of force and non-force entities; conditions, circumstances and influences within which forces employ capabilities to execute joint tasks to meet a specific mission objective". It describes the expected operating environment of the system (or system of systems) under test, and includes all of the elements that influence the required performance that the new 'capability' must demonstrate. These include the particular mission requirements in which the system is being employed; physical factors such as the blue and opposing force structures; geographic and demographic aspects of the joint operating area, etc. as well as the interactions between these elements.

To be successful, testing in the joint environment cannot be a new step added at the end of operational T&E, nor can it replace current developmental or operational testing. It does however represent a departure in the way that DoD Acquisition professionals plan and execute systems engineering, developmental T&E, and operational T&E – indeed the entire acquisition process. Testing in a joint mission environment involves the appropriate combination of representative systems, forces, threats and environmental conditions to support evaluations. These representations can be live, virtual, constructive, or distributed combinations thereof.

Testing in a joint environment applies throughout the life cycle of the system. Identification of a joint issue/problem early in a system's life (including as early as the conceptual phase) will reduce costs and problems. This applies to evaluating system performance, or how well the system does what it is designed to do, as well as the system's contribution to the joint mission, or how we employ the system to achieve the mission. A system's interaction with the joint mission environment is evaluated along an evaluation continuum using constructive and virtual representations and live systems in various combinations.

The joint mission environment and associated joint capability requirements will be defined in the Initial Capabilities Document, Capabilities Development Document, and the Capabilities Production Document. The evaluation plans for assessing these requirements will be articulated in the Systems Engineering Plan (SEP) and the T&E Strategy at Milestone A. At Milestone B and C, they will be articulated in the SEP, TEMP, and Information Support Plan. For each case, the selection of constructive, virtual, and live systems that will be used to recreate the Joint Mission Environment to support testing will depend on the purpose of the assessment and on the interactions the system under test will have with other elements in the joint mission environment.

This section also briefly addresses some additional areas as outlined in the Testing in a Joint Environment Methods and Processes (M&P) Implementation Plan originally produced by the M&P Working Group that was formed during the summer of 2004 to address testing in a joint environment. The areas of concern outlined below are: Description of Joint Mission Environments, How to use the Joint Mission Environment, Testing in a Joint Mission Environment Program Management Office Support, and Important Acquisition Program Responsibilities.

9.9.8.1. Description of Joint Mission Environments

The Joint Capabilities Integration and Development System (JCIDS) will create requirements for effects and capabilities at the joint mission level. This means that JCIDS will identify desired mission level effects that are shortfalls. Shortfalls are addressed by materiel and non-materiel solutions. Materiel or possible system (for a new/modified system or system-of-systems) key performance parameters (KPPs) are then proposed to provide the desired mission level effect(s). Because of this, systems development should not begin and testing cannot occur without definition(s) of the joint mission environment and a defined joint mission associated with a shortfall to be addressed by a system or systems.

With respect to obtaining information for selected joint missions, users of the joint environment can start with the universal joint planning process to break down missions, but it is a process that starts at the Universal Joint Task List (UJTL) level and extends down to the Combatant Command (COCOM) level to plan joint task force operations and/or training events. However, this level of "fidelity" may not be available at the JCIDS Initial Capabilities Document/Capability Development Document/Capability Production Document level, or from Joint Forces Command in that it is mission specific at the COCOM or Joint Task Force level.

The joint mission descriptions should set the stage for evaluation of a system(s) within a joint mission and provide the tester what they need to know to plan the test. There are essential elements of the joint mission description necessary to plan, execute, and analyze assessments and test and evaluation throughout a system's acquisition process.

Additionally, users of the joint environment determine and obtain representations for the threat, threat composition and disposition, and threat scheme of maneuver appropriate for the selected joint mission/task. The currently-approved Guidance for the Development of the Force (GDF) scenarios and/or the maturing Defense Planning Scenarios should be the source of this information. There is also a Threat Scenarios Group from the Test and Evaluation Management Agency working threat scenarios. In addition, coordination with the Service intelligence agencies and the Defense Intelligence Agency is critical. The threat must be system specific (specific to the platform under examination) and also mission specific (specific to the joint mission examined). The next step (after identification of the threat scenarios) is to determine what should be used to represent the threat. This can be a live, virtual, or constructive representation. Threat representations (and others) are addressed as an objective in the Defense Modeling and Simulation Office (DMSO) drafted DoD Modeling and Simulation (M&S) Master Plan.

Different Services should be referred to depending on the type of model that is needed for test. As the Services have generally focused their modeling efforts based on their usual area of operations. The Army and/or the National Geospatial-Intelligence Agency are the best sources for all terrain models. The Navy is the best source for all oceanographic (surface and subsurface) models, and the Air Force is the best source for air and space models. DoD M&S responsibilities are delineated in DoD Directive 5000.59 and there are M&S Executive Agents with responsibilities defined by the DMSO. There should also be a standard set of environment/background models established for the joint mission environment.

9.9.8.2. How to use the Joint Mission Environment

Systems engineering and testing will require insertion of concepts and systems into the joint mission environment as a standard part of the acquisition process. Since this is a change of scope for previous assessments and tests, a process of how to use the joint mission environment has to be established.

The ultimate goal for systems engineering and testing in a joint environment is the ability to insert any system into the applicable joint mission environment at any time during the life of a

system. Two basic items will be examined through insertion into the joint mission environment. The first is to ensure the systems to be acquired are interoperable with other systems. This includes not only how they interact and communicate as expected and required, but also understanding system-of-system dependencies. The second item goes beyond the system interaction and communications to examine what value the systems add to joint military capabilities. In other words, the second item is to assess the contribution of the system to the mission success.

Interoperability and contribution should be examined each time a system is inserted into the joint mission environment and when substantive changes or upgrades are made to an individual system. Users can determine which joint mission/task(s) to test for a system with a role in multiple missions.

Selection of the most stressing mission(s) and/or the mission(s) with the most interactions appears to be the most defensible approach. Test authorities must ensure that if another required mission involves a system interaction not included in the "most stressing" mission, that the interaction is tested separately. Examining different joint missions as the system progresses through the acquisition process is also a good approach especially if there appear to be multiple stressing missions. Another option is to consult with the intended joint users (Combatant Command (COCOM) & Service Combatant) and have them define representative mission tasks.

With respect to the criteria/process to determine the appropriate representations (live, virtual, or constructive) of players in each engineering, development test, or operational test event; the supporting players that constitute the family-of-systems for the joint mission will have to be determined on a case-by-case basis. The goal is for the system being inserted into the joint mission environment to be the most mature representation available. It will always be a live system for Initial Operational Test and Evaluation.

9.9.8.3. Joint Mission Environment (JME) Program Management Office Support

A management and scheduling capability must exist to assist acquisition managers that use the JME. As part of the Testing in a Joint Environment Roadmap, it is assumed a JME Program Management Office will be created to provide this capability.

Scheduling of the assets in the JME, especially live assets participating in exercises, will be a complex undertaking. Not only will it involve coordination of constructive, virtual and live assets, it will also require coordination of specific missions and acquisition systems schedules; most of which will have fixed decision points where unplanned delays could severely impact production.

Availability of the JME should allow systems to "join in" scheduled events, including exercises, as well as coordinate special events among interested agencies. Even then, the testing will be

done with the full coordination and approval of the exercise/training event either as a participant or on a non-interference basis.

9.9.8.4. Important Acquisition Program Responsibilities

The Joint Capabilities Integration and Development System process will necessitate the use of the joint environment and will impact responsibilities for the acquisition program in three basic areas: perspective, assessments, and products.

- The impact in the area of perspective is the addition of a joint mission view to the normal system view.
- The assessment impact reflects that requirements will be stated in terms of system and mission level measures.
- The impact to products is due to the increased emphasis on models and simulation that enables creation of the joint environment for different joint missions. This means constructive and virtual representations of the system must now be created, delivered, and also maintained throughout the life of the system.

9.9.9. Software Test and Evaluation (T&E)

Software is a rapidly evolving technology that has emerged as a major component of most DoD systems. Within the DoD acquisition domain, the following are essential considerations for success in testing software:

- The T&E strategy should address evaluation of highest risk technologies in system design and areas of complexity in the system software architecture. The strategy should identify and describe:
    - Required schedule, materiel and expertise,
    - Software evaluation metrics for Resource Management, Technical Requirements and Product Quality, including Reliability,
    - Types and methods of software testing to support evaluation in unit, integration and system test phases across the life cycle,
    - Data and configuration management methods and tools,
    - Models and simulations supporting software T&E including accreditation status,
- A defined T&E process consistent with and complementing the software and system development, maintenance and system engineering processes, committed to continuous process improvement and aligned to support project phases and reviews, including an organizational and information flow hierarchy.
- Software test planning and test design initiated in the early stages of functional baseline definition and iteratively refined with T&E execution throughout allocated baseline development, product baseline component construction and integration, system qualification and in-service maintenance.

- Software T&E embedded with and complementary to software code production as essential activities in actual software component construction, not planned and executed as follow-on actions after software unit completion.
- Formal planning when considering reuse of Commercial-off-the-shelf or Government-off-the-shelf software, databases, test procedures and associated test data that includes a defined process for component assessment and selection, and test and evaluation of component integration and functionality with newly constructed system elements.
- The following link provides additional information: The Handbook of Software Reliability Engineering, published by IEEE Computer Society Press and McGraw-Hill Book Company (specifically, Chapter 13).

9.9.10. Post Implementation Review (PIR)

Subtitle III of Title 40 of the United States Code (formerly known as Division E of the Clinger-Cohen Act) requires that Federal Agencies ensure that outcome-based performance measurements are prescribed, measured, and reported for Information Technology (including National Security System) programs. DoD Instruction 5000.02 requires that PIRs be conducted for MAIS and MDAP programs in order to collect and report outcome-based performance information. The T&E community will participate in the planning, execution, analysis, and reporting of PIRs, whose results will be used to confirm the performance of the deployed systems and possibly to improve the test planning and execution for follow-on increments or similar systems. For further information, refer to the Acquisition Community Connection or Chapter 7.

9.9.11. System-of-Systems (SoS) Test and Evaluation (T&E)

SoS testing can result in unexpected interactions and unintended consequences. T&E of SoS must not only assess performance to desired capability objectives, but must also characterize the additional capabilities or limitations due to unexpected interactions. The SoS concept should include the system in the broadest sense, from mission planning to sustainment. SoS is a new and evolving area for development, acquisition, and T&E. For further information refer to the Systems Engineering Guide for Systems of Systems.

9.9.12. Reliability Growth Testing

Reliability growth testing supports improvements in system and component reliability over time through a systematic process of stressing the system to identify failure modes and design weaknesses. The emphasis in reliability growth testing is in finding failure modes. The reliability of the system is improved, or experiences growth, as the design is modified to eliminate failure modes. The reliability growth testing approach is sometimes referred to as Test-Analyze-Fix-Test (TAFT). A successful reliability growth program depends on a clear understanding of the intended mission(s) for the system, including the stresses associated with each mission and mission durations, and configuration control. Reliability growth testing should be a part of every

development program and used to provide input to predicted sustainment needs and the reliability KSA. In addition, the results should be used in developing a realistic product support package. For further information, see the DoD Guide for Achieving Reliability, Availability, and Maintainability and associated template.

9.10. Test and Evaluation Master Plan (TEMP) Recommended Format

The recommended TEMP format for all programs, regardless of Acquisition Category, is available as a Word document. While this format is not mandatory, the downloadable document reflects staff expectations. Programs beyond Milestone B using another TEMP format may continue that format or convert to this format at the discretion of the Program Manager. The inclusion of all information shown is required for programs on the OSD Test and Evaluation oversight list. This new format applies to new programs, programs that are being restructured, and any other program at their discretion.

DEFENSE ACQUISITION GUIDEBOOK
Chapter 10 -- Decisions, Assessments, and Periodic Reporting

10.0. Overview

10.0.1. Purpose

This Chapter discusses major program decisions, assessments, and periodic reporting. Generically, it prepares the Program Manager and Milestone Decision Authority to execute their respective oversight responsibilities.

10.0.2. Contents

The chapter starts with overviews of the major decision points and executive reviews associated with a program. It also discusses Integrated Product Teams (IPTs). Other topics include Exit Criteria, Independent Assessments, Information Sharing and Department of Defense (DoD)

Oversight, Management Control, Program Plans, and Periodic Reports. The chapter closes with an overview of the Defense Acquisition Management Information Retrieval System and a discussion of Special Interest Programs. It includes recent changes resulting from the implementation of P.L. 11-23, the Weapon Systems Acquisition Reform Act (WSARA) of 2009.

10.1. Decision Points

10.1.1. Types of Decision Points

There are two types of decision points: milestone decisions and other decision points. Each decision point results in a decision to initiate, continue, advance, change direction in, or terminate a project or program work effort or phase. The review associated with each decision point typically addresses program progress and risk, affordability, program trade-offs, acquisition strategy updates, and the development of exit criteria for the next phase or effort. The type and number of decision points should be tailored to program needs. The Milestone Decision Authority approves the program structure, including the type and number of decision points, as part of the acquisition strategy.

Milestone decisions initiate programs and authorize entry into the major acquisition process phases: Materiel Solution Analysis; Technology Development; Engineering and Manufacturing Development (EMD); and Production & Deployment. The statutory and regulatory information requirements specified in DoD Instruction 5000.02 support milestone decisions.

Decision reviews assess progress and authorize (or halt) further program activity. The regulatory information required to support both milestone decision points and decision reviews should be tailored to support the review, but must be consistent witht he requirements specified in DoD Instruction 5000.02.

10.1.2. Decision Point Certifications

The Milestone Decision Authority for an MDAP signs a certification memorandum for record prior to Milestone A as specified in DTM 09-27, "Implementation of the Weapon Systems Acquisition Reform Act of 2009".

10.1.2.1 Milestone A Certification Requirements

A major defense acquisition program may not receive Milestone A approval until the Milestone Decision Authority certifies, after consultation with the Joint Requirements Oversight Council on matters related to program requirements and military needs, to the following, without modification, from 10 USC 2366a, as amended by Public law 111-23, "Weapon Systems Acquisition Reform Act of 2009", May 22, 2009:

1. that the program fulfills an approved initial capabilities document;
2. that the program is being executed by an entity with a relevant core competency as identified by the Secretary of Defense;
3. an analysis of alternatives has been performed consistent witht he study guidance developed by the Director of Cost Assessment and Program Evalutation;
4. a cost estimate for the program has been submitted, witht he concurrence of the Director of Cost Assessment and Program Evaluation, and the level of resources required to develop and procure the program is consistent witht he priority level assigned by the Joint Requirements Oversight Council; and
5. *[only include if the system duplicates a capability already provided by an existing system]* the duplication provided by this system and (name of existing system) program is necessary to appropriate.

Figure 1. Sample Required Statement for Milestone Decision Authority Certification Memorandum Prior to Milestone A Approval

MEMORANDUM FOR THE RECORD

SUBJECT: Milestone A Certification for _____ Program

As required by section 2366a of title 10, United States Code, I have consulted with the Joint Requirements Oversight Council (JROC) on matters related to program requirements and military needs for the *(name of program)* and certify that:

(1) the program fulfills an approved initial capabilities document;

(2) the program is being executed by an entity with a relevant core competency as identified by the Secretary of Defense;

(3) an analysis of alternatives has been performed consistent with the study guidance developed by the Director of Cost Assessment and Program Evaluation;

(4) a cost estimate for the program has been submitted, with the concurrence of the Director of Cost Assessment and Program Evaluation, and the level of resources required to develop and procure the program is consistent with the priority level assigned by the JROC; and.

(5) *[only include if the system duplicates a capability already provided by an existing system]* the duplication of capability provided by this system and (name of existing system) is necessary and appropriate.

10.1.2.2 Milestone B Certification Requirements

A major defense acquisition program may not receive a Milestone B approval until the Milestone Decision Authority certifies, without modification, from 10 USC 2366b of title 10, United States Code and as amended by Public Law 111-23, "Weapon Systems Acquisition Reform Act of 2009", May 2009, that:

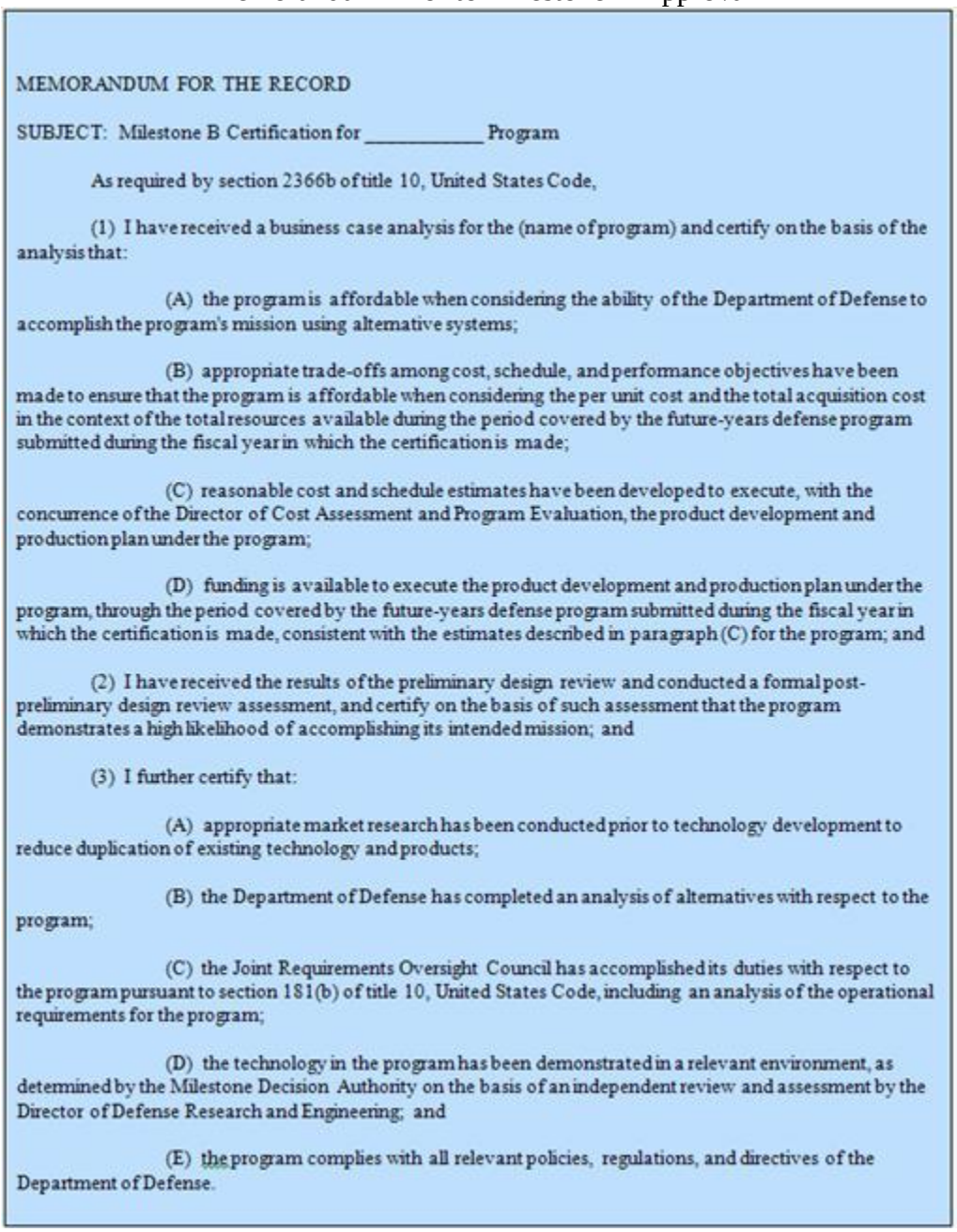
1. I have received a business case analysis and certifies on the basis of the analysis that:
    A. the program is affordable when considering the ability of the Department of Defense to accomplish the program's mission using alternative systems;
    B. appropriate tradeoffs among cost, schedule, and performance objectives have been made to ensure that the program is affordable when considering the per unit cost and total acquisition cost in the context of the total resources available during the period covered by the future-years defense program submitted during the fiscal year in which the certification is made;

C. reasonable cost and schedule estimates have been developed to execute, with the concurrence of the Director of Cost Assessment and Program Evaluation, the product development and production plan under the program;
D. funding is available to execute the product development and production plan under the program, through the period covered by the future-years defense program submitted during the fiscal year in which the certification is made, consistent with the estimates described in subparagraph (C) for the program; and

2. I have received the results of the preliminary design review an conducted a fomal post-preliminary design review assessment, and certify on the basis of such assessment that the program demonstrates a high liklihood of accomplishing its intended mission; and
3. I further certify that:

A. appropriate market research has been conducted prior to technology development to reduce duplication of existing technology and products:
B. the Department of Defense has completed an analysis of alternatives with respect to the program;
C. the Joint Requirements Oversight Council has accomplished its duties with respect to the program pursuant to section 181(b) of title 10 United States Code, including an analysis of the operational requirements for the program;
D. the technology in the program has been demonstrated in a relevant environment as determined by the Milestone Decision Authority on the basis of an independent review and assessment by the direcor of Defense Research and Engineering; and the program complies with all relevant policies, regulations, and directives of the Department of Defense.

Figure 2. Sample Required Statement for Milestone Decision Authority Certification Memorandum Prior to Milestone B Approval



MEMORANDUM FOR THE RECORD

SUBJECT: Milestone B Certification for _____ Program

As required by section 2366b of title 10, United States Code,

(1) I have received a business case analysis for the (name of program) and certify on the basis of the analysis that:

(A) the program is affordable when considering the ability of the Department of Defense to accomplish the program's mission using alternative systems;

(B) appropriate trade-offs among cost, schedule, and performance objectives have been made to ensure that the program is affordable when considering the per unit cost and the total acquisition cost in the context of the total resources available during the period covered by the future-years defense program submitted during the fiscal year in which the certification is made;

(C) reasonable cost and schedule estimates have been developed to execute, with the concurrence of the Director of Cost Assessment and Program Evaluation, the product development and production plan under the program;

(D) funding is available to execute the product development and production plan under the program, through the period covered by the future-years defense program submitted during the fiscal year in which the certification is made, consistent with the estimates described in paragraph (C) for the program; and

(2) I have received the results of the preliminary design review and conducted a formal post-preliminary design review assessment, and certify on the basis of such assessment that the program demonstrates a high likelihood of accomplishing its intended mission; and

(3) I further certify that:

(A) appropriate market research has been conducted prior to technology development to reduce duplication of existing technology and products;

(B) the Department of Defense has completed an analysis of alternatives with respect to the program;

(C) the Joint Requirements Oversight Council has accomplished its duties with respect to the program pursuant to section 181(b) of title 10, United States Code, including an analysis of the operational requirements for the program;

(D) the technology in the program has been demonstrated in a relevant environment, as determined by the Milestone Decision Authority on the basis of an independent review and assessment by the Director of Defense Research and Engineering; and

(E) the program complies with all relevant policies, regulations, and directives of the Department of Defense.

10.2. Executive Reviews

10.2. Executive Reviews

The following paragraphs address DoD assessment reviews associated with major decision points.

10.2.1. Defense Acquisition Board (DAB) Review

The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L)) is the Milestone Decision Authority (MDA) for Acquisition Category (ACAT) ID programs and ACAT IAM programs that have not been delegated. The USD(AT&L) conducts DAB Reviews for ACAT ID and IAM programs at major milestone decision points, at the Full-Rate Production Decision Review (if not delegated), at Interim Program Reviews, and at other times as necessary. Whenever possible, these reviews should take place in the context of the existing Integrated Product Team and acquisition milestone decision review processes. An Acquisition Decision Memorandum (ADM) documents the decision(s) and program direction resulting from the review. Any memorandum the USD(AT&L) signs concerning ACAT ID or IAM programs is referred to as an ADM and should be staffed by the DAB Executive Secretary.

The USD(AT&L) is the Defense Acquisition Executive (DAE). However, since the USD (AT&L) chairs the DAB, and the DAB provides the forum for USD(AT&L) review of ACAT ID and selected IAM programs, ACAT ID and IAM program reviews should be referred to as "DAB Reviews" or "DAB Meetings" and not "DAE Reviews."

The DAB is also the principal review forum enabling the USD(AT&L) to fulfill 10 USC Chapter 144 responsibilities concerning ACAT ID Major Defense Acquisition Programs. The use of any other forum for USD(AT&L) review of ACAT ID programs is discouraged.

DAB members are the following executives: the Vice Chairman of the Joint Chiefs of Staff; the Secretaries of the Military Departments; Under Secretary of Defense (Policy); Under Secretary of Defense (Comptroller); Under Secretary of Defense (Personnel & Readiness); Under Secretary of Defense (Intelligence); Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer; Director, Operational Test & Evaluation; Director, Program Analysis & Evaluation; and Director, Acquisition Resources & Analysis (as the DAB Executive Secretary).

Defense Acquisition Board advisors include the Assistant Secretary of Defense (Acquisition); Assistant Secretary of Defense (Logistics & Material Readiness); Deputy Under Secretary of Defense (Installations and Environment); DoD Deputy General Counsel (Acquisition & Logistics); Director, Defense Research & Engineering; DoD Component Acquisition Executives; the relevant OIPT Leader(s); Director, National Geospatial-Intelligence Agency; Deputy

Director, Cost Assessment; Director, Defense Procurement & Acquisition Policy; Director, Systems Engineering, Director, Developmental Test & Evaluation; Director, Industrial Policy; Director International Cooperation; Assistant Secretary of Defense (Legislative Affairs); Commander, United States Joint Forces Command; Chair, Functional Capabilities Board(s); Cognizant Program Executive Officer(s) and Program Manager(s). The USD(AT&L) may ask other department officials to participate in reviews, as required.

10.2.2. Information Technology Acquisition Board (ITAB)

The ITAB is the decision forum for Milestone review of ACAT IAM programs, excluding defense business systems. The ITAB contributes strategic-level insight for net-centric, global information grid (GIG), and information technology issues when they cannot be resolved at the Overarching Integrated Product Team level. The ITAB facilitates execution of the Milestone Decision Authority's acquisition-related responsibilities for Information Technology, including National Security Systems, under title 10 and subtitle III of title 40 of the United States Code (formerly known as the Clinger-Cohen Act). ITAB Reviews should focus on key principles such as:

- Support of mission needs as described in the Strategic Planning Guidance and the Joint Programming Guidance, Joint Vision 2020, the DoD Information Management and Information Technology Strategic Plan 2008 - 2009, the operational view of the approved Global Information Grid (GIG) Integrated Architecture, and the approved Global Information Grid (GIG) Capstone Requirements Document; And,
- Compliance with the Department of Defense Enterprise Architecture (DoD EA).

An Acquisition Decision Memorandum (ADM) documents the decision(s) resulting from the review.

The USD(AT&L) (or designee, if the program has been delegated) chairs the ITAB. ITAB members are the following department officials: the Information Technology Overarching Integrated Product Team Leader; Cognizant Program Executive Officer(s) and Program Manager(s); Cognizant OSD Principal Staff Assistant(s); the Under Secretary of Defense (Comptroller); the Under Secretary of Defense (Personnel & Readiness);the Director, Operational Test & Evaluation; the Director, Program Analysis and Evaluation; the Director, Force Structure (J8); the Component Acquisition Executives of the Army, Navy, and Air Force; DoD Deputy General Counsel (Acquisition & Logistics); the Director, Systems and Software Engineering; and DoD Component User Representatives.

ITAB advisors include the Under Secretary of Defense (Policy); the Office of the Under Secretary of Defense (Intelligence); the Deputy Under Secretary of Defense (Science and Technology); the Capability Portfolio Manager; the Assistant Secretary of Defense (Legislative Affairs); Component CIOs; the Chairman, OSD Cost Analysis Improvement Group; the Director, Defense Procurement & Acquisition Policy; Representatives of the Joint Staff; the Deputy Under Secretary of Defense (Logistics and Material Readiness); the Deputy Under

Secretary of Defense (Installations and Environment); the Deputy Under Secretary of Defense (Industrial Policy); the Director, International Cooperation; representatives of the DoD Agencies; and the Director, Acquisition Resources & Analysis.

The Milestone Decision Authority may ask other Department officials to participate in reviews when appropriate.

10.2.3. Joint Requirements Oversight Council (JROC)

The JROC reviews and approves capabilities documents designated as JROC interest and supports the acquisition review process. In accordance with the CJCS Instruction 3170.01, the Joint Staff reviews all Joint Capabilities Integration and Development System (JCIDS) documents and assigns a Joint Potential Designator. The JROC validates capability needs. The JROC also validates the key performance parameters when it approves the associated capabilities document. The JROC charters Functional Capabilities Boards. The boards are chaired by a JROC-designated chair and, for appropriate topics, co-chaired by a representative of the Milestone Decision Authority. Functional Capabilities Boards are the lead coordinating bodies to ensure that the joint force is best served throughout the JCIDS and acquisition processes. The JCIDS process encourages early and continuous collaboration with the warfighter and acquisition communities to ensure that new capabilities are conceived and developed in the joint warfighting context. The JROC, at its discretion, may review any JCIDS issues which may have joint interest or impact. The JROC will also review programs at the request of, and make recommendations as appropriate to, the Secretary of Defense, Deputy Secretary of Defense, Under Secretary of Defense (Acquisition, Technology, and Logistics), and the Assistant Secretary of Defense (Networks and Information Integration).

10.2.4. DoD Component Program Decision Review Processes

The OSD-level decision review processes discussed in this section deal specifically with ACAT ID and ACAT IAM programs and selected Pre-Major Defense Acquisition Programs/Pre-Major Automated Information System Programs. DoD Component Acquisition Executives will develop tailored procedures that meet statutory intent for programs under their cognizance.

10.3. Role of Integrated Product Teams (IPTs)

10.3. Role of Integrated Product Teams (IPTs)

Defense acquisition works best when all of the DoD Components work together. Cooperation and empowerment are essential. Per DoD Directive 5000.01, the Department's acquisition community shall implement the concepts of Integrated Product and Process Development (IPPD) and IPTs as extensively as possible (See Rules of the Road: A Guide for Leading Successful Integrated Product Teams).

IPTs are an integral part of the Defense acquisition oversight and review process. For ACAT ID and IAM programs, there are generally two levels of IPTs: the Working-Level Integrated Product Team (WIPT) and the Overarching Integrated Product Team (OIPT). Each program should have an OIPT and at least one WIPT. WIPTs should focus on a particular topic such as cost/performance, program baseline, acquisition strategy, test and evaluation, or contracting. An Integrating Integrated Product Team (IIPT), which is itself a WIPT, should coordinate WIPT efforts and cover all topics not otherwise assigned to another IPT. IPT participation is the primary way for any organization to participate in the acquisition program. IIPTs are essential for ACAT ID and IAM programs, in that they facilitate OSD Staff-level program oversight and review of MDAPs and MAIS programs at the program level. A program "comes together" at the IIPT level and provides the requisite input to the OIPT. The acquisition community should adhere to IPT/IIPT/OIPT terminology and procedures in its program oversight and review role.

10.3.1. Overarching IPT (OIPT) Procedures and Assessment

All Acquisition Category (ACAT) ID and IAM programs will have an OIPT to provide assistance, oversight, and review as the program proceeds through its acquisition life cycle. An appropriate official within OSD, typically the Director, Portfolio Systems Acquisition, the Deputy Assistant Secretary of Defense (DASD) for Command, Control, Communications, Intelligence, Surveillance and Reconnaissance and Information Technology (C3ISR & IT) Acquisition, or the Director, Space and Intelligence Capabilities, will lead the OIPT for ACAT ID programs. The DASD(C3ISR and IT Acquisition) also leads the OIPT for ACAT IAM programs. The OIPT for ACAT IAM programs is called the NII OIPT. OIPTs should include the Program Manager, Program Executive Officer, DoD Component Staff, Joint Staff, and OSD staff involved in oversight and review of the particular ACAT ID or IAM program. Other OIPTs, such as Chem Bio, will be led by similar executives.

The OIPT should form upon departmental intention to start an acquisition program. The OIPT charters the IIPT and WIPT(s). The OIPT should consider the recommendations of the IIPT regarding the appropriate milestone for program initiation and the minimum information needed for the program initiation milestone review. OIPTs should meet thereafter, as necessary, over the life of the program. The OIPT leader should act to resolve issues when requested by any member of the OIPT, or when so directed by the Milestone Decision Authority. The goal is to resolve as many issues and concerns at the lowest level possible, and to expeditiously escalate issues that need resolution at a higher level. The OIPT should bring only the highest-level issues to the Milestone Decision Authority for decision.

At a minimum, the OIPT should normally convene 2 weeks before a planned decision point. It should assess the information and recommendations that the Milestone Decision Authority will receive. It should also assess family-of-system or system-of-system capabilities within and between functional portfolios (or areas) in support of integrated architectures developed by the Joint Staff in collaboration with the OSD Staff and the DoD Components. If the program includes a pilot project, such as Total Ownership Cost Reduction, the Program Manager should report the status of the project to the OIPT. The OIPT should then assess progress against stated goals. The Program Manager's briefing to the OIPT should address interoperability and supportability (including spectrum supportability) with other systems, anti-tamper provisions, and indicate whether those requirements will be satisfied by the acquisition strategy under review. If the program is part of a family-of-systems architecture, the Program Manager should brief the OIPT in that context. If the architecture includes less than ACAT I programs that are key to achieving the expected operational capability, the Program Manager should also discuss the status of and dependence on those programs. The OIPT should review the programmatic issues of cost, schedule, and performance, including risk. The OIPT should review the status of all high and serious risk category ESOH risks and applicable safety technology requirements (see section 4.4.7.6 for specific reporting procedures). The OIPT leader should recommend to the Milestone Decision Authority whether the anticipated review should go forward as planned.

For ACAT ID decision points, the OIPT leader will provide the Defense Acquisition Board chair, principals, and advisors with an integrated assessment using information gathered through the IPPD process. The OIPT assessment should focus on core acquisition management issues and should consider independent assessments, including technology readiness assessments, which the OIPT members normally prepare. These assessments typically occur in context of the OIPT review, and should be reflected in the OIPT leader's report. There should be no surprises at this point - all team members should work issues in real time and should be knowledgeable of their OIPT leader's assessment. OIPT and other staff members should minimize requirements for the program manager to provide pre-briefs independent of the OIPT process.

For ACAT IAM decision points, the OIPT leader will provide the Information Technology Acquisition Board chair, co-chair, principals, and advisors with an integrated assessment using information gathered through the IPPD process, unless the program is a business system.

10.3.2. IIPT and WIPT Procedures, Roles, and Responsibilities

The program manager, or designee, in collaboration with the OSD action officer from the office of the OIPT Leader for the assigned program, should collaborate to form and co-lead an IIPT to support the development of strategies for acquisition and contracts, cost estimates, evaluation of alternatives, logistics management, training, cost-performance trade-offs, etc. The program manager and OSD action officer, assisted by the IIPT, should develop a WIPT structure and propose the structure to the OIPT. The IIPT coordinates the activities of the WIPTs and reviews issues they do not address. WIPTs should meet as required to help the program manager plan program structure and documentation and resolve issues. While there is no one-size-fits-all WIPT approach, the following basic tenets should apply:

- The program manager is in charge of the program.
- WIPTs are advisory bodies to the program manager.
- Direct communication between the program office and all levels in the acquisition oversight and review process is expected as a means of exchanging information and building trust.

The program manager or the program manager's representative should normally lead each WIPT. The following roles and responsibilities should apply to all WIPTs:

- Assist the program manager in developing strategies and in program planning.
- Propose tailored documentation and milestone requirements.
- Review and provide early input to acquisition documents.
- Coordinate activities with the OIPT members.
- Resolve or elevate issues in a timely manner.
- Assume responsibility to obtain principals' concurrences on issues, documents, or portions of documents.

IPTs are critical to program success, and training is critical to IPT success. All IPT members should receive general IPT procedural training. The Acquisition Community Connection web site has additional information about WIPTs.

10.3.3. Industry Participation

Industry representatives may be invited to a WIPT or IIPT meeting to provide information, advice, and recommendations to the IPT; however, the following policy should govern their participation:

- Industry representatives will not be formal members of the IPT.
- Industry participation will be consistent with the Federal Advisory Committee Act.
- Industry representatives may not be present during IPT deliberations on acquisition strategy or competition sensitive matters, nor during any other discussions that would give them a marketing or competitive advantage.
- At the beginning of each meeting, the IPT chair should introduce each industry representative, including their affiliation, and their purpose for attending.
- The chair should inform the IPT members of the need to restrict discussions while industry representatives are in the room, and/or the chair should request the industry representatives to leave before matters are discussed that are inappropriate for them to hear.
- Support contractors may participate in WIPTs and IIPTs, but unless specifically authorized by the organization they represent, they may not commit the staff organization they support to a specific position. The organizations they support are responsible for ensuring the support contractors are employed in ways that do not create the potential for a conflict of interest. Contractors supporting staff organizations may participate in Overarching Integrated Product Team (OIPT) discussions; however, they will not be

permitted to represent the position of the supported organization and they may be asked to sign non-disclosure statements prior to deliberations.

Given the sensitive nature of OIPT discussions, industry representatives and support contractors may not be permitted to participate in certain OIPT discussions. However, the OIPT leader may permit contractors to make presentations to the OIPT, when such views will better inform the OIPT and will not involve the contractors directly in Government decision making.

10.4. Role of Exit Criteria

Milestone Decision Authorities should use exit criteria for ACAT I and ACAT IA programs during an acquisition phase. Prior to each milestone decision point and at other decision reviews, the program manager, in collaboration with the IPT, will develop and propose exit criteria appropriate to the next phase or effort of the program. The OIPT will review the proposed exit criteria and make a recommendation to the Milestone Decision Authority. Exit criteria approved by the Milestone Decision Authority will be published in the ADM.

System-specific exit criteria normally track progress in important technical, schedule, or management risk areas. Unless waived, or modified by the Milestone Decision Authority, exit criteria must be satisfied for the program to continue with additional activities within an acquisition phase or to proceed into the next acquisition phase (depending on the decision with which they are associated). Exit criteria should not be part of the Acquisition Program Baseline (APB) and are not intended to repeat or replace APB requirements or the phase-specific entrance criteria specified in DoD Instruction 5000.02. They should not cause program deviations. **Status of approved exit criteria will be reported in the Defense Acquisition Executive Summary.**

10.5. Role of Independent Assessments

10.5. Role of Independent Assessments

Assessments, independent of the developer and the user, provide a different perspective of program status. However, requirements for independent assessments (for example, Program Support Reviews, Assessments of Operational Test Readiness, the independent cost estimate, or technology readiness assessment) must be consistent with statutory requirements, policy, and good management practice. Senior acquisition officials should consider these assessments when making acquisition decisions. Staff offices that provide independent assessments should support the orderly and timely progression of programs through the acquisition process. IPT access to independent assessments, to provide unbiased program perspectives, facilitates full and open discussion of issues.

10.5.1. Independent Cost Estimate

Section 101 of Public Law 111-23, "Weapon Systems Acquisition Reform ACt of 2009", May 22, 2009, requires the Director, Cost Assessment and Program Evaluation (DCAPE) to conduct independent cost esimates (ICEs) on Major Defense Acquisition Programs (MDAPs) for which the USD(AT&L) is the MDA, and also, in certain circumstances, for Major Automated Information Systems (MAIS) programs. The statute also requires DCAPE to review DoD Component cost estimates and cost analyses conducted in connection with Major Defense Acquisition Programs (MDAPS).

Additionally, DCAPE is required to provide policies and procedures for the conduct of all DoD cost estimates (and issues guidance relating to the full consideration of life-cycle management and sustainabiliy costs).

10.5.1.1. Independent Cost Estimate (ICE) for MDAPs

The DCAPE conducts independent cost estimates (ICEs) and cost analyses for MDAPs for which the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) is the MDA in advance of:

(1) Any decision to enter low rate initial production (LRIP), or full rate production (FRP).

(2) Any certification pursuant to sections 2366a, 2366b, or 2433a of title 10, United

States Code.

(3) At any other time considered appropriate by the DCAPE or upon the request

of the USD(AT&L).

10.5.1.2. Independent Cost Estimate (ICE) for MAIS Programs

The DCAPE, conducts independent cost estimates (ICEs) and cost analyses for MAIS programs for which the USD(AT&L) is the MDA in advance of:

(1) Any report pursuant to section 2445c(f) of title 10, United States Code.

(2) At any other time considered appropriate by the DCAPE or upon the request of the

USD(AT&L).

10.5.1.3. Review of Cost Estimates

The DCAPE participates in the discussion of any discrepancies related to MDAP and MAIS cost estimates, comments on deficiencies regarding the methodology or the execution of the estimates, concurs with the choice of the cost estimate used to support the acquisition program baseline (APB) or any of the cost estimates identified in paragraphs 10.5.1.1. and 10.5.1.2, and participates in the consideration of any decision to request authorization of a multi-year procurement contract for a MDAP.

10.5.1.4. Cost Estimate Confidence Levels

The DCAPE and the Secretary of the Military Department concerned or the head of the Defense Agency concerned (as applicable) state the confidence level used in establishing the cost estimate for MDAP and MAIS programs, provides the rationale for selecting the confidence level, and, if the confidence level is less than 80 percent, the justification for selecting the lower confidence level. The confidence level statement shall be included in the ADM approving the APB, and in any other cost estimates for MDAPs or MAIS programs prepared in association with the estimates identified in paragraphs 10.5.1.1. and 10.5.1.2. For MDAPs, the confidence level statement shall also be included in the next selected acquisition report (SAR) prepared in compliance with section 2432 of title 10, United States Code, and for MAIS, in the next quarterly report prepared in compliance with section 2445c of title 10, United States Code.

10.5.2. Technology Maturity and Technology Readiness Assessments

Technology maturity is a measure of the degree to which proposed critical technology elements (CTEs) meet program objectives; and, is a principal element of program risk. A technology readiness assessment examines program concepts, technology requirements, and demonstrated technology capabilities in order to determine technological maturity. The program manager should identify critical technologies, using tools such as the Work Breakdown Structure. In order to provide useful technology maturity information to the acquisition review process, technology readiness assessments of CTEs and identification of critical program information (CPI) must be completed prior to Milestone Decision points B and C.

P.L. 111-23, the Weapon Systems Acquisition Reform Act of 2009, requires the Director of Defense Research and Engineering (DDR&E) to develop knowledge-based standards againstwhich to measure the technological maturity and integration risk of critical technologies at key stages in the acquisition process for the purpose of conducting the required reviews and assessments of MDAPs.

10.5.2.1. Assessment of MDAP Technologies

The DDR&E independently reviews, assesses, and reports the maturity of MDAP technologies to the MDA prior to MS B certification.

10.5.2.2. Technology Readiness Levels (TRLs)

A summary table of TRL descriptions, Table 10.5.2.T1 follows:

Technology Readiness Level	Description
1. Basic principles observed and reported.	Lowest level of technology readiness. Scientific research begins to be translated into applied research and development. Examples might include paper studies of a technology's basic properties.
2. Technology concept and/or application formulated.	Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies.
3. Analytical and experimental critical function and/or characteristic proof of concept.	Active research and development is initiated. This includes analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.
4. Component and/or breadboard	Basic technological components are integrated to

validation in laboratory environment.	establish that they will work together. This is relatively "low fidelity" compared to the eventual system. Examples include integration of "ad hoc" hardware in the laboratory.
5. Component and/or breadboard validation in relevant environment.	Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so it can be tested in a simulated environment. Examples include "high fidelity" laboratory integration of components.
6. System/subsystem model or prototype demonstration in a relevant environment.	Representative model or prototype system, which is well beyond that of TRL 5, is tested in a relevant environment. Represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high-fidelity laboratory environment or in simulated operational environment.
7. System prototype demonstration in an operational environment.	Prototype near, or at, planned operational system. Represents a major step up from TRL 6, requiring demonstration of an actual system prototype in an operational environment such as an aircraft, vehicle, or space. Examples include testing the prototype in a test bed aircraft.
8. Actual system completed and qualified through test and demonstration.	Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation of the system in its intended weapon system to determine if it meets design specifications.
9. Actual system proven through successful mission operations.	Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation. Examples include using the system under operational mission conditions.

Table 10.5.2.T1. TRL Descriptions

The use of TRLs enables consistent, uniform, discussions of technical maturity across different types of technologies. Decision authorities will consider the recommended TRLs (or some equivalent assessment methodology, e.g., Willoughby templates) when assessing program risk. TRLs are a measure of technical maturity. They do not discuss the probability of occurrence (i.e., the likelihood of attaining required maturity) or the impact of not achieving technology maturity.

For additional information, see the on-line TRA Deskbook.

10.5.3. Preliminary Design Review (PDR) Review and Assessment

P.L. 111-23, the Weapon Systems Acquisition Reform Act of 2009, has established conduct of PDR before MS B as a mandatory requirement for all MDAPs. The Program Manager (PM) shall plan a Preliminary Design Review (PDR); PDR planning shall be reflected in the TDS, details should be provided in the SEP, and shall be conducted consistent with the policies specified in DoD Instruction 5000.02. and the plan for PDR will be reflected in the Technology Development Strategy (TDS) to be approved by the MDA at MS A. Post-PDR assessments will be conducted in association with MS B preparations and will be formally considered by the MDA at the MS B 2366b certification review.

PDRs before MS B for other than MDAPs will be approved by the MDA when consistent with TDS or Acquisition Strategy objectives. When the PDR is conducted before MS B, a post-PDR assessment will be conducted in association with the MS B review and formally considered by the MDA at the MS B review. If the PDR is conducted after MS B, the MDA will conduct a post-PDR assessment at a time reflected in the approved acquisition strategy.

If a PDR has not been conducted prior to Milestone B (non-MDAPs), the PM shall plan for a PDR as soon as feasible after program initiation. PDR planning shall be reflected in the Acquisition Strategy and conducted consistent with the policies specified in paragraph 5.d.(6) of DoD Instruction 5000.02.

10.5.3.1. Preliminary Design Review (PDR) Report

The PDR Report shall be provided as a memorandum to the MDA. When the USD(AT&L) is the MDA for a program, the PDR Report should b provided by a memorandum to the USD(AT&L), with copies to the Director, Systems Engineering and OIPT Leader.

The PDR Report shoul dinclude:

a. A comprehensive list of the systems engineering products that make up the allocated baseline (to include the preliminary design specifications for all configuration items) and that were subject to review;
b. A list of the participants in the review including the PDR chair, applicable technical authorities, independent subject matter experts, and other key stakeholders;
c. A summary of the action Items from the review and their closure status/plan;
d. A risk assessment using the PDR risk assessment checklist or similar, and preliminary Environment, Safety, and Occupational Health hazard lists/assessments to determine readiness to commit to full detail design; and
e. A recommendation from the PDR as to the approval of the program's system allocated baseline to support detail design.

The Preliminary Design Review (PDR) Report shall be provided to the MDA prior to Milestone B and include recommended technical requirements trades based upon an assessment of cost,

schedule, and performance risk.

10.5.4. Post-Preliminary Design Review (Post-PDR) Assessment Decision Review

When the system-level PDR is conducted after Milestone B (non-MDAPs), the PM shall plan and the MDA shall conduct a formal Post-PDR Assessment Decision Review. The MDA shall conduct a formal program assessment and consider the results of the PDR and the PM's assessment in the PDR Report, and determine whether remedial action is necessary to achieve APB objectives. The results of the MDA's Post-PDR Assessment shall be documented in an ADM. The Post-PDR assessment shall reflect any requirements trades based upon the PM's assessment of cost, schedule, and performance risk.

10.5.5. Post-Critical Design Review (Post-CDR) Assessment

The MDA shall conduct a formal Post-CDR Assessment Decision Review following the system-level CDR.

1. The PM shall provide a Post-CDR Report to the MDA as a memorandum that provides an overall assessment of design maturity and a summary of the system-level CDR results which shall include, but not be limited to:
    a. The names, organizations, and areas of expertise of independent subject matter expert participants and CDR chair;
    b. A description of the product baseline for the system and the percentage of build-to packages completed for this baseline;
    c. A summary of the issues and actions identified at the review together with their closure plans;
    d. An assessment of risk by the participants against the exit criteria for the EMD Phase; and
    e. Identification of those issues/risks that could result in a breach to the program baseline or substantively impact cost, schedule, or performance.

The CDR risk assessment checklist is designed as a technical review preparation tool, and should be used as the primary guide for assessing risk during the review. This checklist is available on the Systems Engineering COP.

2. When the USD(AT&L) is the MDA for a program, the Post-CDR Report should be provided by a memorandum to the USD(AT&L), with copies to the Director, Systems and Software Engineering and the OIPT leader.
3. The MDA shall review the Post-CDR Report and the PM's resolution/ mitigation plans and determine whether additional action is necessary to satisfy EMD Phase exit criteria and to achieve the program outcomes specified in the APB. The results of the MDA's Post-CDR Assessment Decision Review shall be documented in an ADM staffed by the

DAB Executive Secretary.

10.6. Information Sharing and DoD Oversight

10.6.1. Program Information

It is DoD policy to keep reporting requirements to a minimum. Nevertheless, complete and current program information is essential to the acquisition process. Consistent with the tables of required regulatory and statutory information in DoD Instruction 5000.02; decision authorities require program managers and other participants in the defense acquisition process to present the minimum information necessary to understand program status and make informed decisions. The Milestone Decision Authority "tailors-in" program information case-by-case, as necessary. IPTs facilitate the management and exchange of program information.

The program manager, the DoD Component, or the OSD staff prepares most program information. Some information requires approval by an acquisition executive. Other information is for consideration only. In most cases, information content and availability are more important than format.

Unless otherwise specified (e.g., Defense Acquisition Management Information Retrieval (DAMIR), Selected Acquisition Report (SAR), Acquisition Program Baseline, and Defense Acquisition Executive Summary (DAES)> submissions), Program Managers may use stand-alone documents or a single document to submit mandatory information. If the program manager submits stand-alone documents, the program manager should minimize redundancy and not include the same information in each document. Unless otherwise specified, all plans, waivers, certifications and reports of findings referred to in this Guidebook are exempt from licensing under one or more exemption provisions of DoD 8910.1-M.

10.6.2. Life-Cycle Management of Information

Program managers will comply with record keeping responsibilities under the Federal Records Act for the information collected and retained in the form of electronic records (See DoD Directive 5015.2. Electronic record keeping systems should preserve the information submitted, as required by 44 U.S.C. 3101, and implementing regulations. Electronic record keeping systems should also provide, wherever appropriate, for the electronic acknowledgment of electronic filings that are successfully submitted. Program managers must consider the record keeping functionality of any systems that store electronic documents and electronic signatures to ensure

users have appropriate access to the information and can meet the Agency's record keeping needs.

10.6.3. Classification and Management of Sensitive Information

Program managers must review their programs to identify and document critical program information (CPI) requiring protection (DoD Instruction 5200.39). Program managers must also review their programs to identify controlled unclassified information (CUI). (CUI includes "FOUO" information as defined in DoD Directive 5230.24 and information with other approved markings requiring dissemination controls that are exempt from mandatory disclosure under the Freedom of Information Act (e.g., DoD 5400.7-R, DoD Directive 5230.25, and Export Control Act).

When necessary, program managers develop Security Classification Guides> in accordance with DoD 5200.1-R.

10.7. Management Control

Program managers will implement internal management controls in accordance with DoD Directive 5000.01 and DoD Instruction 5000.02. APB parameters serve as control objectives. Program managers normally identify deviations from approved APB parameters and exit criteria as material weaknesses. Program managers must focus on results, in consonance with most efficient and effective processes. Program managers must ensure that obligations and costs comply with applicable law. Further, they must safeguard assets against waste, loss, unauthorized use, and misappropriation; properly record and account for expenditures; maintain accountability over assets; and quickly correct identified weaknesses.

10.8. Program Plans

Program plans describe the detailed activities of the acquisition program. Except as specified by DoD Instruction 5000.02, the program manager (in coordination with the Milestone Decision Authority and Program Executive Officer) should determine the type and number of program plans needed to manage program execution.

10.9. Periodic Reports

10.9. Periodic Reports

Periodic reports include only those reports required by the Milestone Decision Authority or statute. Except for the reports outlined in this section, the Milestone Decision Authority tailors the scope and formality of reporting requirements.

10.9.1. Statutory Reporting

10.9.1.1. Revised MDAP Definition

P. L. 111-23, "Weapons Systems Acquisition Reform Act of 2009," May 22, 2009, revised the definition of a Major Defense Acquisition Program (MDAP) as follows. A MDAP is a DoD acquisition program that is not a highly sensitive classified program and:

(1) That is designated by the USD(AT&L) as a MDAP; or

(2) That is estimated to require an eventual total expenditure for research, development, test, and evaluation, INCLUDING ALL PLANNED INCREMENTS, of more than $365 million (based on fiscal year 2000 constant dollars) or an eventual total expenditure for procurement, INCLUDING ALL PLANNED INCREMENTS, of more than $3.19 billion (based on fiscal year 2000 constant dollars).

10.9.1.2. Designation of Subprograms for MDAPs

10.9.1.2.3. Prohibition on Obligations (Subprograms)

The National Defense Authorization Act (NDAA) for FY 2009 amended Chapter 144 of title 10 (section 2430a), United States Code, to give the Department authority to designate subprograms within Major Defense Acquisition Programs (MDAPs).

The Secretary of Defense (delegated to the USD(AT&L)) may designate subprograms within an MDAP. That is, when an MDAP requires the delivery of two or more categories of end items that differ significantly in form and function, subprograms may be established for base-lining and reporting purposes. The law stipulates that when one subprogram is designated within an MDAP, all remaining elements (increments or components) of the program shall also be appropriately organized into one or more other subprograms.
In the DoD acquisition environment, there are two primary instances when establishing subprograms within an MDAP may be advisable:

1. The first instance is a product of evolutionary acquisition when increments or blocks of capability are acquired in a sequential manner. With subprogram reporting, each of these increments can be baselined and tracked separately for cost (including unit cost), schedule, and performance purposes within a single MDAP without the risk of artificial cost growth or a Nunn-McCurdy breach when subsequent increment is initiated. In accordance with DoDI 5000.02, each evolutionary increment must have its own Milestone B (or Milestone C if initiated at production) and its own Acquisition Program Baseline (APB). The requirement for a separate APB for each evolutionary increment is satisfied through the establishment of an APB containing subprograms. An example of this type of subprogram is the block upgrade of a missile system that provides significant increases in altitude and/or range.

2. The second instance is when there are major components of a program that are dissimilar and therefore cannot be combined in a rational way to produce a unit cost that is representative of the program. An example is the use of separate subprograms for satellites and ground-based receivers to improve visibility and unit cost reporting.

The decision whether to establish subprograms for an MDAP requires careful analysis and must be made on a case-by-case basis. Structuring an MDAP with subprograms should reflect the way the program is being managed, and represent the most efficient and informative way to convey information about a program to senior defense acquisition officials as well as to Congress. For Acquisition Category (ACAT) ID MDAPs, the DAE will approve the designation of subprograms based on recommendations from the Overarching Integrated Product Team (OIPT). For ACAT IC MDAPs, the authority to designate subprograms is delegated to the respective DoD Component Milestone Decision Authority (MDA). In either case, the recommendations from the OIPT or the MDA staff should also include appropriate guidance on how the relevant statutory and regulatory requirements of DoD Instruction 5000.02 should apply at the subprogram or program level (for example, how to

structure the acquisition strategy or the independent cost estimate for a program with designated subprograms).

10.9.1.2.1. Subprogram Notification

The law requires that the SECDEF (delegated to USD(AT&L) must notify the congressional defense committees in writing of any proposed subprogram designation not less than 30 days before the date such designation takes effect. The approval of an APB reflecting such designation will be considered the date that subprogram designation takes effect; therefore, notification to Congress must occur not less than 30 days before a subprogram APB is approved.

Accordingly, DoD Components must notify the Director, Acquisition Resources and Analysis of all proposed APBs that reflect new or revised subprogram designations at least 60 days before the proposed APB is submitted to the MDA for approval. Once a subprogram structure is established for an MDAP, the Defense Acquisition Executive Summary (DAES), Selected Acquisition Report (SAR), and Nunn-McCurdy Unit Cost Reports (quarterly and breach) will reflect that subprogram structure.

10.9.1.2.2. Subprogram Critical Cost Growth

In the event a subprogram experiences critical unit cost growth, the certification required for the program to continue will be made at the program level—not the subprogram level.

10.9.1.2.3. Prohibition on Obligations (Subprograms)

The prohibition on obligations until the submission of the SAR for significant breaches, and the certification for critical breaches, will affect all major contracts of the program, not just those relating to the breaching subprogram.

10.9.1.3. Acquisition Program Baseline (APB) Reporting

10.9.1.3.1. Program Deviations

The program manager must maintain a current estimate of the program being executed (see definition of "current estimate" in section 10.9.1.3.2, below). The program manager must immediately notify the Milestone Decision Authority when a baseline deviation occurs based

upon the current estimate. A baseline deviation occurs when the current estimate is "beyond" the threshold. (See section 2.1.1 and 10 USC 2433.)

10.9.1.3.2. Current Estimate

The current estimate is the latest estimate of program acquisition cost and quantity, schedule milestone dates, performance characteristic values, and critical technical parameters of the approved program (i.e., the approved program as reflected in the currently approved APB, ADM, or in any other document containing a more current decision of the MDA or other approval authority). For cost, the current estimate is normally the President's Budget plus or minus known changes; for schedule, it is normally the program manager's best estimate of current schedule milestone dates; for performance it is normally the program's manager's best estimate of current performance characteristics values.

Program managers will report the current estimate of each APB parameter periodically to the Milestone Decision Authority. The MDA will direct the frequency of the reporting. PMs will report current estimates for ACAT I and IA programs quarterly in the DAES.

10.9.1.3.3. Program Deviation Reporting

When the program manager has reason to believe that the current estimate for the program indicates that a performance, schedule, or cost threshold value will not be achieved, he or she will immediately notify the MDA of the deviation. Within 30 days of the occurrence of the program deviation, the program manager will submit a Program Deviation Report to the MDA providing the reasons for the program deviation and the actions that need to be taken to bring the program back within the baseline parameters (if this information was not included with the original notification). Within 90 days of the occurrence of the program deviation, one of the following should have occurred: the program is back within APB parameters; a new APB (changing only those parameters that were breached) has been approved; or an OIPT-level or equivalent Component-level review has been conducted to review the program manager's proposed baseline revisions and make recommendations to the Milestone Decision Authority regarding the parameters that were breaches. The MDA will decide, based on criteria in 10 USC 2433 and 2435, whether it is appropriate to approve a revision to the APB.

If one of the above actions has not occurred within 90 days of the program deviation, the USD(AT&L) for ACAT ID programs, or if delegated, the ASD(NII) for ACAT IAM programs, or the CAE for ACAT IC and/or ACAT IAC programs, should hold a formal program review to determine program status.

10.9.1.4. Selected Acquisition Report (SAR)

10.9.1.4. Selected Acquisition Report (SAR)

In accordance with 10 U.S.C. 2432, the Secretary of Defense will submit a SAR to Congress for all MDAPs. The program manager will use the Defense Acquisition Management Information Retrieval (DAMIR) application to prepare the SAR.

10.9.1.4.1. SAR Content and Submission

The SAR reports the status of total program cost, schedule, and performance, as well as program unit cost and unit cost breach information. Each SAR will include a full life-cycle cost analysis for the reporting program, each of its evolutionary increments, as available, and for its antecedent program, if applicable.

The SAR for the quarter ending December 31 is the annual SAR. The program manager will submit the annual SAR within 60 days after the President transmits the following fiscal year's budget to Congress. Annual SARs will reflect the President's Budget and supporting documentation. The annual SAR is mandatory for all ACAT I programs.

The program manager will submit quarterly exception SARs for the quarters ending March 31, June 30, and September 30 not later than 45 days after the quarter ends. Quarterly SARs are reported on an exception basis, as follows:

- The current estimate exceeds the Program Acquisition Unit Cost (PAUC) objective or the Average Procurement Unit Cost (APUC) objective of the currently approved APB in base-year dollars by 15 percent or more;
- The current estimate includes a 6-month or greater delay, for any schedule parameter, that occurred since the current estimate reported in the previous SAR;
- Milestone B or Milestone C approval occurs within the reportable quarter.

Quarterly exception SARs will report the current estimate of the program for cost, schedule, and performance (see definition of current estimate in section 10.9.1.3.2, above).

Pre-Milestone B projects may submit RDT&E-only reports, excluding procurement, military construction, and acquisition-related operations and maintenance costs. DoD Components should notify USD(AT&L) with names of the projects for which they intend to submit RDT&E-only SARs 30 days before the reporting quarter ends. USD(AT&L) should also notify Congress 15 days before reports are due.

Whenever USD(AT&L) proposes changes to the content of a SAR, he or she will submit notice of the proposed changes to the Armed Services Committees of the Senate and House of Representatives. USD(AT&L) may consider the changes approved, and incorporate them into the report, 60 days after the committees receive the change notice.

Per section 206, WSARA 2009, for MDAPs certified subsequent to a critical cost breach, the first SAR for the program submitted after the President submits a budget in the calendar year following the year in which the program was restructured must include a description of all funding changes made as a result of the growth in cost of the program, including reductions made in funding for other programs to accommodate such cost growth.

Per section 2366b of title 10, U.S.C., the SAR for any MDAP receiving a waiver for one or more MS B certification criteria must prominently and clearly indicate that such program has not fully satisfied the certification requirements for MS B, until such time that the MDA makes a determination that the program has satisfied all such certification requirements.

10.9.1.4.2. SAR Waivers

In accordance with 10 U.S.C. 2432, the Secretary of Defense may waive the requirement for submission of a SAR for a program for a fiscal year if:

- The program has not entered EMD;
- A reasonable cost estimate has not been established for the program; and,
- The system configuration for the program is not well defined.

As delegated by the Secretary of Defense, USD(AT&L) will submit a written notification of each waiver for a fiscal year to the Armed Services Committees of the Senate and House of Representatives not later than 60 days before the President submits the budget to Congress, pursuant to 31 U.S.C. 1105, in that fiscal year. However, with the transition to the Milestone A-B-C Acquisition Model (see DoD Instruction 5000.02, Enclosure 2), this waiver authority is rarely employed.

10.9.1.4.3. SAR Termination

USD(AT&L) will consider terminating SAR reporting when 90 percent of expected production deliveries or planned acquisition expenditures have been made, or when the program is no longer considered an ACAT I program in accordance with 10 U.S.C. 2432.

10.9.1.5. Unit Cost Reports (UCR)

10.9.1.5. Unit Cost Reports (UCR)

In accordance with 10 U.S.C. 2433, the program manager will prepare UCRs for all ACAT I programs submitting SARs, except pre-Milestone B programs that are reporting RDT&E costs only.

10.9.1.5.1. Unit Cost Report (UCR) Content and Submission

The program manager will report the unit costs of the program to the CAE on a quarterly basis through the electronic Defense Acquisition Executive Summary (DAES) submission process. The program manager should submit the update in accordance with DAES submission procedures. Reporting should begin with submission of the initial SAR, and terminate with submission of the final SAR. Each report should include the current estimate of the Program Acquisition Unit Cost and the Average Procurement Unit Cost (in base-year dollars); cost and schedule variances, for each of the major contracts since entering the contract; and all changes that the program manager knows or expects to occur to program schedule or performance parameters, as compared to the currently approved Acquisition Program Baseline.

10.9.1.5.2. Unit Cost Report (UCR) Breach Reporting

10.9.1.5.2.1. Significant Cost Growth Notification Requirements

The program manager will notify the CAE immediately, whenever there is a reasonable cause to believe that the current estimate of either the Program Acquisition Unit Cost (PAUC) or Average Procurement Unit Cost (APUC) (in base-year dollars) has increased by 15 percent (or more) over the PAUC or APUC objective of the currently approved Acquisition Program Baseline, respectively, or 30 percent (or more) over the PAUC or APUC of the original/revised original APB.

If the CAE determines that there is an increase in the current estimate of the PAUC or APUC of at least 15 percent over the currently approved APB, the CAE should inform USD(AT&L) and the cognizant Head of the DoD Component. If the cognizant Head of the DoD Component subsequently determines that there is, in fact, an increase in the current estimate of the PAUC or APUC of at least 15 percent over the currently approved APB, the Head of the DoD Component will notify Congress, in writing, of a breach. The notification will be not later than 45 days after

the end of the quarter, in the case of a quarterly report; or not later than 45 days after the date of the report, in the case of a report based on reasonable cause. In either case, notification will include the date that the Head of the DoD Component made the determination. In addition, the Head of the DoD Component will submit a SAR for either the fiscal year quarter ending on or after the determination date, or for the fiscal year quarter that immediately precedes the fiscal year quarter ending on or after the determination date. This SAR should contain the additional, breach-related information.

10.9.1.5.2.2. Critical Cost Breach Certification Requirements

Public Law 111-23, "Weapon Systems Acquisition Reform Act of 2009," May 22, 2009, added section 2433a of title 10, United States Code resulting in changes to actions that must be taken following critical cost growth of a MDAP or designated subprogram.

The PM shall notify the DoD component acquisition executive (CAE) immediately, whenever there is a reasonable cause to believe that the current estimate of either the program acquisition unit cost (PAUC) or average procurement unit cost (APUC) of a MDAP or designated subprogram (in base-year dollars) has increased by 25 percent (or more) over the PAUC or APUC objective of the currently approved APB estimate, or 50 percent (or more) over the PAUC or APUC of the original APB estimate.

If the CAE determines that there is an increase in the current estimate of the PAUC or APUC of at least 25 percent over the PAUC or APUC objective of the currently approved APB, or 50 percent over the PAUC or APUC of the original APB, the CAE shall inform the USD(AT&L) and the cognizant Head of the DoD Component. If the cognizant Head of the DoD Component subsequently determines that there is, in fact, an increase in the current estimate of the PAUC or APUC of at least 25 percent over the currently approved APB, or 50 percent over the PAUC or APUC of the original APB, the Head of the DoD Component shall notify Congress, in writing, of the determination of critical cost growth and the increase with respect to the program or subprogram concerned. The notification shall be not later than 45 days after the end of the quarter, in the case of a quarterly report; or not later than 45 days after the date of the report, in the case of an out-of-cycle report based on critical change occurring between quarters. In either case, notification shall include the date that the Head of the DoD Component made the determination. In addition, the Head of the DoD Component shall submit a SAR for either the fiscal year quarter ending on or after the determination date, or for the fiscal year quarter that immediately precedes the fiscal year quarter ending on or after the determination date. This SAR shall contain the additional critical cost growth-related information.

Additionally, the USD(AT&L), after consultation with the JROC regarding program requirements, shall determine the root cause or causes of the critical cost growth in accordance with applicable statutory requirements and DoD policies, procedures, and guidance based upon the root cause analysis conducted by the senior official for PARCA; and in consultation with the DCAPE, shall carry out an assessment of:

a. The projected cost of completing the program if current requirements are not modified.
b. The projected cost of completing the program based on reasonable modification of such requirements.
c. The rough order of magnitude of the costs of any reasonable alternative system or capability.
d. The need to reduce funding for other programs due to the growth in cost of the program.

After conducting the reassessment, the USD(AT&L) shall terminate the program unless The USD(AT&L) submits a written certification to Congress before the end of the 60-day period beginning on the day the SAR containing the unit cost information is required to be submitted to Congress. The certification must state:

a. The continuation of the program is essential to the national security.
b. There are no alternatives to the program that will provide acceptable capability to meet the joint military requirement (as defined in section 181(g) of section 2366a of title 10, United States Code) at less cost.
c. The new estimates of the PAUC or APUC have been determined by the DCAPE, to be reasonable.
d. The program is a higher priority than programs whose funding must be reduced to accommodate the growth in cost of the program.
e. The management structure for the program is adequate to manage and control PAUC or APUC.

The written certification shall be accompanied by a report presenting the root cause analysis and assessment and the basis for each determination made in accordance with the five certification criteria listed in paragraphs 5.a. through 5.e. of this section, and supporting documentation.

If the USD(AT&L) elects NOT to terminate a MDAP that has experienced critical cost growth, the Secretary of Defense shall:

a. Restructure the program in a manner that addresses the root cause or causes of the critical cost growth, as identified by the actions described above, and ensure that the program has an appropriate management structure as set forth in the written certification;
b. Rescind the most recent milestone approval for the program or designated subprograms and withdraw any associated certification(s) pursuant to section 2366a or 2366b of title 10, United States Code.
c. Require a new milestone approval for the program or designated subprograms before taking any contract action to enter a new contract, exercise an option under an existing contract, or otherwise extend the scope of an existing contract under the program, except to the extent determined necessary by the MDA, on a non-delegable basis, to ensure that the program can be restructured as intended by the Secretary of Defense without unnecessarily wasting resources.
d. Include in the report a description of all funding changes made as a result of the growth in cost of the program, including reductions made in funding for other programs to

accommodate such cost growth. (The report specified here is the first SAR for the program submitted after the President submits a budget in the calendar year following the year in which the program was restructured.)

Additionally, for each MDAP that has exceeded the critical cost thresholds, but has not been terminated, the Director, Program Assessment and Root Cause Analysis (PARCA) shall conduct semi-annual reviews until 1 year after the date a new milestone approval is received. The Director, PARCA, shall report the results of the semi-annual reviews to the USD(AT&L) and summarize the results in the Director's next annual report.

If a MDAP is terminated after experiencing a critical cost breach, the USD(AT&L) shall submit to Congress a written report with the following information:

a. An explanation of the reasons for terminating the program.
b. The alternatives considered to address any problems in the program.
c. The course the Department of Defense plans to pursue to meet any continuing joint military requirements otherwise intended to be met by the program.

10.9.1.5.2.3. Restriction on Obligation of Funds

If the Head of the DoD Component makes a determination of either a PAUC or APUC increase of 15 percent or more and a SAR containing the additional unit cost breach information is not submitted to Congress as required, or if the Head of the DoD Component makes a determination of a 25 percent increase or more in the PAUC or APUC and a certification by the USD(AT&L) is not submitted to Congress as required, funds appropriated for RDT&E, procurement, or military construction may not be obligated for a major contract under the program. An increase in the PAUC or APUC of 25 percent or more resulting from the termination or cancellation of an entire program will not require USD(AT&L) program certification.

10.9.1.6. Performance Assesments and Root Cause Analysis (PARCA)

The Director, PARCA is a newly established position to execute specified responsibilities. Per section 103 of Public Law 111-23, “Weapon Systems Acquisition Reform Act of 2009, May 22, 2009, the senior official for PARCA shall:

(1) Conduct performance assessments for MDAPs periodically or when requested by the Secretary of Defense, the USD(AT&L), the Secretary of a Military Department, or the head of a Defense Agency. Performance assessments shall evaluate the cost, schedule, and performance of the program, relative to current metrics, performance requirements, and baseline parameters. The assessments shall determine the extent to which the level of program cost, schedule, and performance relative to established metrics is likely to result in the timely delivery of a level of capability to the warfighter. The capability should be consistent with the level of resources to be expended and provide superior value to alternative approaches that may be available to meet the same requirement.

(2) Conduct root cause analyses for MDAPs as required by section 2433a of title 10, United States Code, or when requested by the Secretary of Defense, the USD(AT&L), the Secretary of a Military Department, or the head of a Defense Agency. Root cause analysis shall consider the underlying cause or causes for shortcomings in cost, schedule, and performance including the role, if any, of unrealistic performance expectations; unrealistic baseline estimates for cost and schedule; immature technologies or excessive manufacturing or integration risk; unanticipated design, engineering, manufacturing, or integration issues arising during program performance; changes in procurement quantities; inadequate program funding or funding instability; poor performance by government or contractor personnel responsible for program management; or any other matters.

(3) Shall advise acquisition officials on performance issues regarding a MDAP that may arise:

(a) Prior to certification pursuant to section 2433a of title 10, United States Code.

(b) Prior to entry into full-rate production.

(c) In the course of consideration of any decision to request authorization of a

multiyear procurement contract.

(4) Shall work with the DCAPE and other DoD officials in the conduct of performance

10.9.2. Major Automated Information System (MAIS) Statutory Reporting

The FY07 National Defense Authorization Act (NDAA), Section 816, instituted a reporting regime requiring MAIS programs to prepare and submit annual and quarterly reports. This was codified in title 10 U.S.C. Chapter 144A, and has been amended several times.

Briefly, the statute defines dollar thresholds for Major Automated Information System (MAIS) programs and other investments required to report. A MAIS Annual Report (MAR) is due to the congressional defense committees 45 days after submission of the President's Budget, and each quarter a MAIS Quarterly Report (MQR) is due to "a senior Department of Defense official responsible for a MAIS program," hereafter referred to as the Senior Official.

The statute also describes required reports due to the congressional defense committees if a Program Manager (PM) estimates a Significant or Critical Change. As shown in table 10.9.2.T1, below, Significant and Critical Changes can occur in performance, schedule, and/or cost.

	Significant	**Critical**

Cost (program development cost or total life-cycle cost)	15-25% increase	≥ 25% increase
Schedule	>6 month - 1 year delay	≥ 1 year delay
		Failed to achieve FDD within 5 yrs after funds were first obligated for the program (see section 10.9.2.5.2.1)
Performance	Significant adverse change in expected performance	Undermine the ability of the system to perform mission as originally intended (miss a KPP)
Report to congressional defense committees	Notification due 45 Days after office of Senior Official receives MQR	Program Evaluation and Report due 60 days after office of Senior Official receives MQR

Table 10.9.2.T1. Significant and Critical Changes

If a Significant Change to a program is determined by the Senior Official, the requirement to send the congressional defense committees a Notification within 45 days is triggered. Determination of a Critical Change, however, will initiate the requirement to conduct an Evaluation of the program and send a Report (with certifications) to Congress within 60 days. If the Report is not submitted within the 60-day period, appropriated funds may not be obligated for any major contract under the program. This prohibition ends on the day on which the congressional defense committees receive a report in compliance with the statute.

For additional information please see the Chapter 144A Definitions and Rarely Asked Questions. A complete copy of this Chapter 144A implementation guidance is also available.

10.9.2.1. Programs Required to Report

10.9.2.1. Programs Required to Report

As amended, 10 U.S.C. Ch 144A requires annual and quarterly reports from MAIS programs, pre-MAIS programs, and "any other investment in automated information system [AIS] products or services that is expected to exceed the [MAIS] thresholds…."

- The MAIS threshold definition is statutory (in Chapter 144A) and explained in Table 1 of DoD Instruction 5000.02:
  - $32 million in fiscal year (FY) 2000 constant dollars for all expenditures, for all increments, regardless of the appropriation or fund source, directly related to the AIS definition, design, development, and deployment, and incurred in any single fiscal year; or
  - $126 million in FY 2000 constant dollars for all expenditures, for all increments, regardless of the appropriation or fund source, directly related to the AIS definition, design, development, and deployment, and incurred from the beginning of the Materiel Solution Analysis Phase through deployment at all sites; or
  - $378 million in FY 2000 constant dollars for all expenditures, for all increments, regardless of the appropriation or fund source, directly related to the AIS definition, design, development, deployment, operations and maintenance, and incurred from the beginning of the Materiel Solution Analysis Phase through sustainment for the estimated useful life of the system.
- As a footnote to Table 1, AIS is defined as "a system of computer hardware, computer software, data or telecommunications that performs functions such as collecting, processing, storing, transmitting, and displaying information. Excluded are computer resources, both hardware and software, that are:

“a. an integral part of a weapon or weapon system;

“b. used for highly sensitive classified programs (as determined by the Secretary of Defense);

“c. used for other highly sensitive information technology programs (as determined by the ASD(NII)/DoD CIO); or

“d. determined by the USD(AT&L) or designee to be better overseen as a non-AIS program (e.g., a program with a low ratio of RDT&E funding to total program acquisition costs or that requires significant hardware development).”

10.9.2.1.1. MAIS Programs

A MAIS Program is defined (in Ch 144A and DoDI 5000.02) as "a DoD acquisition program for an Automated Information System (either as a product or a service) that is either:

- "Designated by the Milestone Decision Authority (MDA) as a MAIS; or
- "Estimated to exceed [one of the MAIS dollar thresholds]."

Increments of a program that separately meet these definitions must also report individually as well as in the aggregate. Increments that are separately baselined and which do not meet or exceed any Chapter 144A MAIS dollar threshold are not required to report under Chapter 144A. For continuity, any such increment should be appropriately described in the MAIS Annual Report Program Description.

According to DoD Directive 5000.01, The Defense Acquisition System, "an Acquisition Program is a directed, funded effort that provides a new, improved, or continuing materiel, weapon or information system or service capability in response to an approved need." The direction and full-funding criteria are generally understood to be satisfied—and a program is "initiated"—at Milestone B approval.

10.9.2.1.2. Pre-MAIS Programs and Other Investments

The amended Ch 144A expands coverage of the reporting requirements to pre-MAIS Programs and other investments in AIS.

- A Pre-MAIS program is defined as "an investment that is designated by the Secretary of Defense, or a designee of the Secretary, as a ‘pre-Major Automated Information System' or 'pre-MAIS' program." Pre-MAIS designations are made by the USD(AT&L) or the MDA.
- The reporting requirements also apply to "any other investment in [AIS] products or services that is expected to exceed the [MAIS thresholds] but is not considered to be a [MAIS] program because a formal acquisition decision has not yet been made with respect to such investment." "Investment" exists after the first occurrence of any of the following events: 1) designation as a pre-MAIS, 2) Milestone (MS) A, or 3) MS B.

10.9.2.1.3. Ending the Requirement to Report; Close-out Reports

Many reasons exist to suggest the need for a program to report under Chapter 144A should not arise or has come to an end. The USD (AT&L) or his designee will make this determination based on consideration of the facts, including:

- the program does not or no longer meets the definitions presented above;
- the program has been terminated; or
- the program has achieved full deployment (FD).

For reporting programs determined to no longer require Chapter 144A reporting, a "close-out" MAIS Annual Report must be completed and submitted to Congress during the next reporting cycle. Similarly, a “close-out” MAIS Quarterly Report must be completed and submitted to the Senior Official when it is next due. Close-out reports must articulate one of the three circumstances above and cite an existing authoritative document (signed by an appropriate

authority) as support. If subsequent increments of a program survive that are below reportable thresholds, note their existence in the close-out report.

10.9.2.2. MAIS Annual Report (MAR)

10.9.2.2. MAIS Annual Report (MAR)

Title 10 U.S.C. Chapter 144A requires the Secretary of Defense to "submit to Congress each calendar year, not later than 45 days after the President submits to Congress the budget … justification documents regarding cost, schedule and performance for each Program Required to Report for which funds are requested by the President in the budget." DoD meets this requirement by compiling for each program a report called the MAIS Annual Report (MAR). Templates and Instructions can be found at Instructions for Preparing the Major Automated Information System (MAIS) Annual Report.

The MAR should be unclassified. If the required information is classified, then the classified data is replaced with the word "CLASSIFIED."

10.9.2.2.1. Preparing the Report

The MAIS Annual Report is prepared by the PM and consists of a PDF document that includes a cover sheet/table of contents, and the following seven sections: Program Information, Points of Contact, Program Description, Program Status, Schedule, Performance Characteristics, and Cost. Report separate performance/schedule/cost data for each increment or block under active acquisition. Do not report increments or blocks that have reported achievement of Full Deployment (FD) in a previous MAR. The Instructions for Preparing the Major Automated Information System (MAIS) Annual Report explain how to prepare the report using the Microsoft Excel workbook and Microsoft Word document provided as templates.

10.9.2.2.2. Submitting the Report

PMs should submit the report to their DoD Component Acquisition Executive (CAE) (or equivalent official) following Component procedures. The CAE's designated representative will then submit the unclassified reports via email to C3ISR_IT_ACQUISITION@OSD.MIL.

Components will submit Final Draft reports as detailed above for Office of Secretary of Defense (OSD)-level review and coordination by the second Friday of January each year. Not later than the second Friday of February, the Office of the Under Secretary of Defense (Acquisition, Technology, and Logistics) (OUSD(AT&L)), the Office of the Assistant Secretary of Defense

(Networks and Information Integration) (OASD(NII)), and the Office of the Deputy Chief Management Officer (ODCMO) will coordinate the OSD-level review and provide feedback to the Components through issue resolution teleconferences held during the second week of February.

Components will submit a Final MAR via a transmittal memo signed by an appropriate SES/flag acquisition official to OASD(NII) not later than the last Friday in February. OASD(NII) will consolidate and submit the final MARs to Congress no later than 45 days after submission of the President's Budget the first Monday in February.

Table 10.9.2.2.2.T1 describes a typical reporting cycle.

Event	Responsible Agency	Typical Target Date
Task Components for MAR cycle	OASD(NII)	10 Dec
Submit final Draft MARs	Components	15 Jan
Review and consolidate feedback to the OSD acquisition analyst	OSD staff	5 Feb
OSD/Component issue resolution teleconferences	OSD & Components	10 Feb
Submit Final MARs together with a transmittal memo	Components	25 Feb
Consolidate, staff, and submit MARs to Congress	OASD(NII)	20 Mar

Table 10.9.2.2.2.T1. Review Cycle Events and Typical Target Dates

10.9.2.3. MAIS Quarterly Report (MQR)

10.9.2.3.1. Reporting Cycle

10.9.2.3.2. MAIS Quarterly Report (MQR) Form and Contents

10.9.2.3.3. Program Manager's Current Estimate

10.9.2.3.4. Senior Official

10.9.2.3.5. Quarterly Report Anticipation and Receipt

10.9.2.3.6. Determinations by the Senior Official

10.9.2.3. MAIS Quarterly Report (MQR)

Title 10 U.S.C. Chapter 144A requires the PM to submit a written MQR to the Senior Official responsible for the program identifying any variance from the projected schedule, life-cycle cost, or key performance parameters as baselined in the MAR. All Programs Required to Report, once having submitted a MAR, will submit MQRs even if they have not experienced any variance from their cost, schedule or performance baseline. MQR guidance was first articulated in the DASD(C3ISR & IT Acquisition) memo "Chapter 144A MAIS Quarterly Report Process" dated 22 April 2008, and it is summarized in the following paragraphs.

10.9.2.3.1. Reporting Cycle

Although a separate report, the MQRs follow the Defense Acquisition Executive Summary (DAES) submission cycle, and bear the same date as the program's DAES. MQRs are due on the last business day of every third month, maintaining the DAES group reporting rotation (see section 10.9.3.1).

10.9.2.3.2. MAIS Quarterly Report (MQR) Form and Contents

For simplicity, the completed MAR should be adapted to create the MQR. Templates and Instructions for the MAR can be found at Instructions for Preparing the Major Automated Information System (MAIS) Annual Report. The adaptation steps are as follows:

- Cover page: Change "MAIS Annual Report" to "MAIS Quarterly Report" and change the "as-of" date to the date of the concurrent DAES.
- Program Information, Points of Contact, or Program Description: Make any corrections or updates.
- Program Status: This section will be used by the PM to identify variances to the Senior Official. Replace the MAR's standard paragraphs with a statement similar to the following: "The following pages reflect the current or actual estimates for cost, schedule and performance as of April xx, 2009. None of the variances from the original estimates meet the Chapter 144A definition of either a Significant or a Critical Change." Or, if any of the reported variances do represent a Significant or Critical Change, the second sentence should so indicate, and continue with a useful explanation. Skillful PMs will provide language here that can be cut and pasted into an ensuing Notification or Critical Change Report to Congress.
- Schedule, Performance and Cost: Continue to use the same information in the Original Estimate columns as presented in the MAR. If, however, a Critical Change Report has resulted in revised program documentation (e.g., APB), update the Original Estimate with the approved estimates. The "Current Estimate or Actual" columns for each of these factors should be updated to reflect the Current Estimate on the as-of-date of the MQR.

10.9.2.3.3. Program Manager's Current Estimate

The Program Manager's Current Estimate is the latest estimate of program acquisition cost and quantity, schedule milestone dates, and performance characteristic values of the approved program (i.e., the approved program as reflected in the currently approved APB, ADM, or in any other document containing a more current decision of the MDA or other approval authority). For cost, the current estimate is normally the President's budget plus or minus fact of life changes. For schedule, the Current Estimate is normally the program manager's best estimate of current schedule milestone dates. For performance, it is normally the PM's best estimate of current performance characteristic values.

10.9.2.3.4. Senior Official

The senior Department of Defense official responsible for a program is:

- The Service Acquisition Executive (SAE) for a program acquired by a Military Department (Army, Navy, or Air Force).
- The USD(AT&L) for a program acquired by a DoD Component other than a Military Department when direct authority (i.e., Milestone Decision Authority) has been retained by the USD(AT&L).
- The Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) for a program acquired by a DoD Component other than a Military Department, unless the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) has retained direct authority. (Note: The USD(AT&L) made this Senior Official delegation to the ASD(NII) in a memorandum "MAIS Programs" dated July 18, 2007.)
- The Deputy Chief Management Officer (DCMO) for defense business system programs delegated in writing by the USD(AT&L).

10.9.2.3.5. Quarterly Report Anticipation and Receipt

PMs are responsible for reporting the execution status of their programs to their acquisition management chain: PEO, CAE, OIPT Leader, MDA, and—for Chapter 144A Quarterly Reports purposes—the Senior Official. If a PM becomes aware the program will experience a variance exceeding a Significant or Critical Change threshold, the PM should immediately notify his/her acquisition management chain, in advance of the due date for the next MAIS Quarterly Report (MQR). Since the MQR is the vehicle for official notification of Significant and Critical changes, the 45- or 60-day deadlines for reporting to Congress are established from the date the MQR is due to the office of the Senior Official (e.g., OASD(NII)), i.e., the last business day of the month the MQR is due.

If determination of a Significant Change is contemplated, the deadline for Notification to Congress is the last business day before 45 days expire.

- If determination of a Critical Change is contemplated, the deadline for conducting a program evaluation and certifying a report of results to Congress is the last business day before 60 days expire.

10.9.2.3.6. Determinations by the Senior Official

The (staff office of a) Senior Official should promptly review an MQR to see whether it reflects a less than "significant" (or no) variance, a "Significant Change," or a "Critical Change" in cost, schedule or performance. Senior Officials may choose to obtain independent opinions on the measurement of a variance and proper determination of a Change.

If none of the reported factors exhibit a variance exceeding a Significant Change threshold, nothing further needs to be done to satisfy the statute.

If a cost, schedule, or performance factor exhibits a variance exceeding a Significant or Critical Change threshold, the Senior Official makes such determination, and proceeds to satisfy the statutory requirements. Model processes are suggested below.

- Significant Change Process.
- Critical Change Process.

10.9.2.4. Significant Changes

10.9.2.4. Significant Changes

If, based on the MAIS Quarterly Report (MQR), the Senior Official makes a determination that a Significant Change has occurred, the Senior Official must, not later than 45 days after receiving the MQR, notify the congressional defense committees in writing of that determination.

10.9.2.4.1. Significant Change Thresholds

A Significant Change is defined as one in which one of the following has occurred:

- There has been a schedule change that will cause a delay of more than 6 months but less than a year in any program schedule milestone or significant event from the schedule submitted as the Original Estimate,

- The estimated program development cost or total life-cycle cost for the program has increased by at least 15 percent, but less than 25 percent, over the Original Estimate, or
- There has been a significant, adverse change in the expected performance from the parameters submitted in the original MAR. The Department, however, has determined that a "significant, adverse change" is defined as a failure to meet a Key Performance Parameter (KPP) threshold value, which is the same definition chosen for a Critical Change in performance (addressed below). Therefore, all such failures will be determined to be Critical Changes.

10.9.2.4.2. Model Significant Change Process

When a Significant Change is determined, the Senior Official must notify the congressional defense committees in writing that he or she has made such Determination. The Determination and Notification (hereafter "Notification") should be in the form of a 1-2 page letter signed by the Senior Official and is due to the congressional defense committees not later than 45 days after the date the MQR was received in the office of the Senior Official. If the Senior Official is a Service Acquisition Executive (SAE), the Notification must also be coordinated with either the USD(AT&L) or the ASD(NII) before sending to Congress.

The Notification should acknowledge that a Significant Change, as defined by the statute, has occurred. Succinctly state the specific factor that has varied in excess of a threshold, the reasons for the variance, and indicate what actions (including reprogramming) the PM has or may take to bring the program back within baseline parameters or avoid further deviation from the baseline. If known, indicate the projected new cost or schedule.

If a Notification has been sent informing the congressional defense committees of a Significant Change in one factor (cost, schedule, or performance), and that factor's variance has expanded (but not exceeded a Critical Change criteria) in a subsequent MQR, no additional Notification need be sent to the congressional defense committees. If, however, a subsequent MQR indicates that a different reporting factor has an over-threshold variance, another Notification must be sent informing the congressional defense committees of this additional basis for a Determination of Significant Change.

10.9.2.4.3. Coordination and Transmittal of a Significant Change Notification to Congress

Notifications are drafted by PMs and coordinated with their PEO and CAE for signature by the Senior Official. By a combination of statute and policy, Notifications from an SAE Senior Official must be coordinated through an OSD office before transmittal to Congress. The one- to two-page Notification letter should be signed by the SAE (acting as a Senior Official) and coordinated with the appropriate OSD official: the USD(AT&L) (when MDA is retained); the DCMO (when the subject program is a delegated defense business system); or the ASD(NII) (in all other cases). At least 5 working days should be allowed for this coordination process. In cases

where the Senior Official is the ASD(NII), DCMO, or USD(AT&L), the CAE should prepare the Notification letter for that OSD official's signature and transmittal. At least 10 working days should be allowed for the review and signature process.

10.9.2.5. Critical Changes

10.9.2.5. Critical Changes

When the Senior Official anticipates or makes a determination that a Critical Change has occurred, the Senior Official should initiate a process to satisfy the statutory and regulatory requirements. This section describes those requirements and sets forth a model process.

10.9.2.5.1. Critical Change Thresholds

A Critical Change is defined by the statute as one in which any of the following has occurred:

- The system failed to achieve a full deployment decision (FDD) within 5 years after funds were first obligated for the program (this threshold and an exception to it are more fully explained in section 10.9.2.5.2, below);
- There has been a schedule change that will cause a delay of one year or more in any program schedule milestone or significant event from the schedule originally submitted to Congress in the MAR;
- The estimated program development cost or full life-cycle cost for the program has increased by 25 percent or more over the original estimate submitted to Congress in the MAR; or
- There has been a change in the expected performance of the MAIS that will undermine the ability of the system to perform the functions anticipated at the time information on the program was originally submitted to Congress in the MAR. The Department has determined that a critical performance change is defined as a failure to meet a KPP threshold value.

10.9.2.5.2. Five-Year-to-FDD Threshold

MAIS programs should be structured so that each Increment can achieve an FDD within five years from when funds are first obligated for the Increment. The program structure and (upon sufficient maturity) the criteria that constitute a Full Deployment Decision, should be reflected in the Increment's Acquisition Strategy or Acquisition Program Baseline.

10.9.2.5.2.1. Failed to Achieve a Full Deployment Decision (FDD)

The phrase "failed to achieve" is interpreted literally; the Increment must have actually exceeded (not expected to exceed) five years between start of the 5-year clock and FDD. A breach of this threshold will therefore be reported in the MQR next due after the 5-year point.

If, however, any other Critical Change is reported in advance of the 5-year point and it is expected that FDD will not occur within the 5-year threshold, include an additional determination of the 5-year-to-FDD breach in the evaluation and report to Congress. When the 5-year point arrives, re-send the report to Congress with a transmittal letter indicating that "the previously reported certifications were meant to apply now."

If there is no reason to determine and report any Critical Change in advance of failure to achieve FDD within 5 years, such determination, evaluation, report, and certification will be accomplished after the 5-year point is reached in accordance with the first paragraph of this section.

For programs that have achieved an FDD (no matter how long it took), that event has overcome the 5-year-to-FDD breach criterion, and it is no longer applicable.

10.9.2.5.2.2. Funds First Obligated Date

The "funds first obligated" date for each Increment is the earliest of the following:

- An ADM that approves a Milestone A;
- An ADM that approves the preferred alternative for an Increment of an unbaselined program. (For example, the MDA could approve in an ADM a preferred alternative based on an Analysis of Alternatives.);
- The date explicitly established in an ADM as a "funds first obligated" date. (For example, if the MDA is concerned that substantial funds are being spent on an IT investment before receiving Milestone A approval, the MDA could designate the investment as an unbaselined MAIS program and explicitly establish in the ADM the date when funds were first obligated.)

10.9.2.5.2.3. Exception for Programs with 2008 MARs

MAIS programs that submitted a MAR in 2008 should maintain the 5-year-to-Initial Operational Capability (IOC) start date included in that MAR to determine when a Critical Change may occur. This exception cannot be extended to any other program, and the 5-year clock will stop upon achievement of IOC (if before October 28, 2009) or an FDD.

10.9.2.5.2.4. Full Deployment Decision (FDD) Date

The FDD is the final Milestone Decision Authority decision authorizing an Increment of an acquisition program to deploy software for operational use. Each Increment can have only one FDD.

If the Increment will have more than one software release, the MDA should specifically designate in an ADM which release fielding decision will serve as the FDD for the entire Increment. (For example, if an Increment has four software releases each having a fielding decision, then one fielding decision should be designated the FDD based on the criteria below. The 5-year development clock stops when the FDD ADM is signed by the MDA.)

A release event would be appropriately designated as the FDD based on the accumulation of successes related to the entire Increment (and specified in the Acquisition Strategy or Acquisition Program Baseline), such as:

- low percentage of total functionality remains to be developed,
- IOT&E indicates that the system is operationally effective, suitable, and survivable,
- high percentage of capability fielded,
- high percent of geographical fielding completed,
- high percentage of legacy system(s) replaced,
- insignificant risk associated with remaining releases, and achievement of Initial Operational Capability.

10.9.2.5.3. Program Evaluation

Upon determination of a Critical Change, the statute directs an evaluation ("E") of the program, including "an assessment of-

- (E1) "the projected cost and schedule for completing the program if current requirements are not modified;
- (E2) "the projected cost and schedule for completing the program based on reasonable modification of such requirements; and
- (E3) "the rough order of magnitude of the cost and schedule for any reasonable alternative system or capability."

While not *per se* a part of the Critical Change Report that will be submitted to the congressional defense committees, these three "E" assessments will feed into the four certification ("C") areas of the Critical Change Report described below.

10.9.2.5.4. Report on Critical Program Changes

The statute further directs delivery of a report (i.e., Critical Change Report (CCR)) to the congressional defense committees, including: "a written certification (with supporting explanation) stating that-

- (C1) "the automated information system or information technology investment to be acquired under the program is essential to the national security or to the efficient management of the Department of Defense;
- (C2) "there is no alternative to the system or information technology investment which will provide equal or greater capability at less cost;
- (C3) "the new estimates of the costs, schedule, and performance parameters with respect to the program and system or information technology investment, as applicable, have been determined, with the concurrence of the Director of Cost Assessment and Program Evaluation, to be reasonable; and
- (C4) "the management structure for the program is adequate to manage and control program costs."

To avoid a prohibition on the obligation of funds for major contracts, the report must be submitted to the congressional defense committees not later than 60 days after the date the MAIS Quarterly Report (MQR) was due to the staff office of the Senior Official.

10.9.2.5.5. Model Critical Change Process

10.9.2.5.5.1. Critical Change Triage Team; Determination and Tasking

In anticipation of, or upon receipt of a MAIS Quarterly Report containing notice of a Critical Change, the staff office of the Senior Official should organize a Triage Meeting to:

- Review the nature and severity of the Change,
- Recommend a complete or abbreviated Critical Change process to the Senior Official, and
- Outline the leadership structure and scope of the Critical Change Team that will conduct the evaluation and prepare a Critical Change Report (CCR). See below for further advice on organizing the CCT and its several Integrated Product Teams (IPTs).

Attending the Triage Meeting should be senior representatives from 1) the staff office of the Senior Official, 2) JCS (J8 Force Structure Resources and Assessment), 3) CAPE (Program Evaluation, and Cost Analysis if USD(AT&L) is the MDA), 4) OUSD(AT&L) (Acquisition Resources & Analysis), and 5) the OSD office with program oversight responsibility (Overarching Integrated Product Team (OIPT), Investment Review Board (IRB), or equivalent).

The staff office will document the advice of the Triage Meeting in a draft "Determination and Tasking" memorandum to be signed by the Senior Official. The "Determination and Tasking" memorandum will:

- state the Senior Official's determination and nature of the Critical Change,
- direct a program evaluation be conducted,
- direct a report of the results be prepared, and
- designate leadership of a Critical Change Team to manage the process.

10.9.2.5.5.2. Critical Change Team (CCT) and Meetings

As part of the "Determination and Tasking" memorandum, the Senior Official should establish leadership for a Critical Change Team (CCT) to conduct the program evaluation and produce the Critical Change Report. A Team Leader from an appropriate oversight or program integration office under the Senior Official will organize the CCT and integrate the contributions of the several IPTs. The Team Leader should be an O-5/O-6 or equivalent civilian. Additionally, a Flag/SES-level "IPT Principals Lead" from the Senior Official's staff should be named to provide advice and direction to the CCT, as well as to chair meetings of a committee of "IPT Principals." Figure 10.9.2.5.5.2.F1. is a notional depiction of CCT Organization and Reporting Paths.

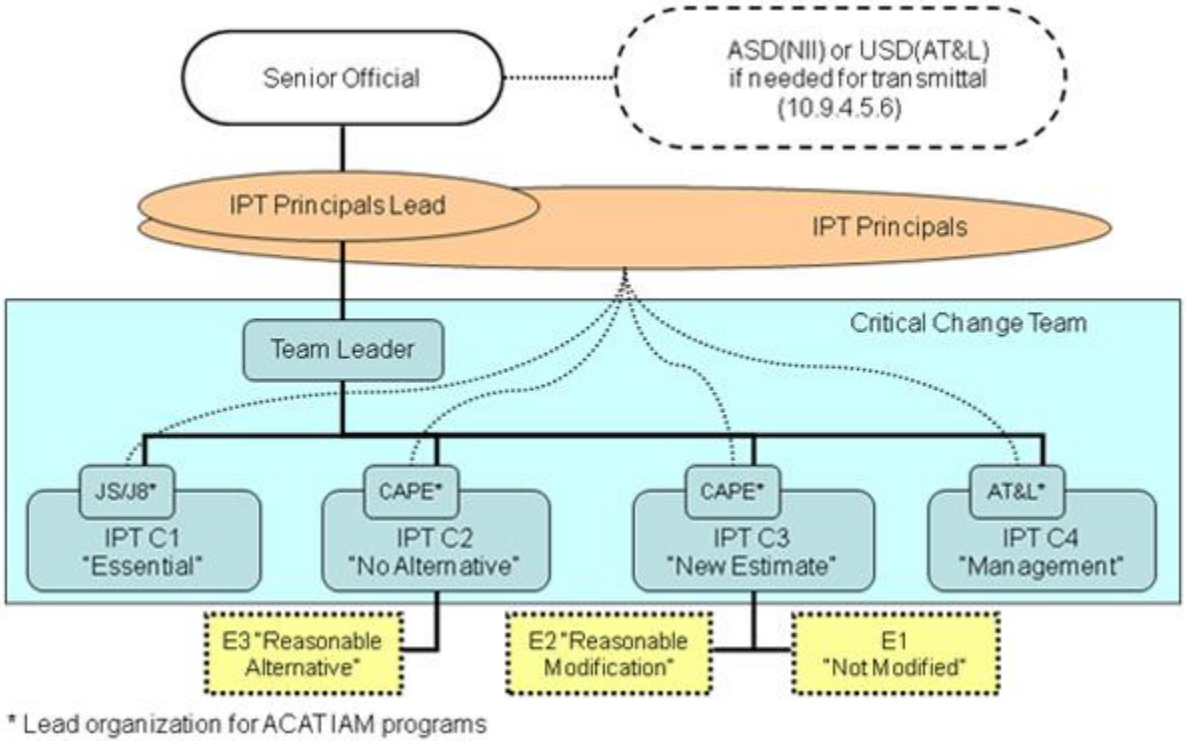


Figure 10.9.2.5.5.2.F1. Critical Change Team (CCT) Organization and Reporting Path

Ultimately, the Senior Official must be satisfied sufficiently with the evaluation and report to sign the certification statements required by the statute. When the Senior Official perceives the need to specify leadership or membership of individual IPTs, that specification should also be made as part of the "Determination and Tasking" memorandum. Otherwise, the IPT Principals Lead and Team Leader will select individual members and leadership of the IPTs that will focus on certifications C1-4. Membership should include all interested parties, and individuals must be empowered to represent their organizations. In all cases, IPT membership and leadership designations should consider joint/departmental interests as well as the circumstances of the Critical Change.

A kickoff meeting of the CCT should be held as soon as possible in anticipation of a Critical Change being determined. The IPT Principals Lead and CCT Leader should guide the organization of the CCT into IPTs and specify expected contributions and a detailed timeline. The CCT (or the Team Leader alone) should meet again with the IPT Principals Lead as necessary, and at least once for a mid-process progress check. Eventually, the CCT should meet to pre-brief the IPT Principals Lead on the final Report. The final Report and briefing should then be presented to the IPT Principals for a final review of the Report before delivery to the Senior Official for certification (signature).

10.9.2.5.5.3. IPT Membership and Focus

The Critical Change process should be conducted by Integrated Product Teams (IPTs) under the CCT, each focused on Certifications 1-4. To preserve IPT and CCT independence, to the maximum extent practicable team membership should be independent of the Program Management Office. IPT membership should be selected to maximize the success of the group and avoid non-productive contributions.

- IPT C1 will document the explanation that permits the Senior Official to certify "the automated information system or information technology investment to be acquired under the program is essential to the national security or to the efficient management of the DoD." The IPT C1 should write a few paragraphs about the need for the program:
    - Include threat, mission, and current systems available to meet the threat or efficient management need.
    - Reference relevant strategy documents, CONOPS, roadmaps, requirements documents, threat assessments, Quadrennial Defense Review, etc.
    - Address the program and the capability to be acquired, as appropriate.
    - *IPT C1 members*: Component operations staff, PEO staff, CAE staff, user representatives, PM, JCS/J8, OSD (PSA and OSD Acquisition Analyst).
- IPT C2 will document the explanation that permits the Senior Official to certify that "there is no alternative to the system or information technology investment which will provide equal or greater capability at less cost." This IPT should:
    - Reference any existing Analysis of Alternatives and discuss any major deviations from past analysis. Do not re-accomplish the Analysis of Alternatives.
    - Identify any alternative systems.
    - Include the assessment (E3) of the "rough order of magnitude of the cost and schedule for any reasonable alternative system or capability."
    - *IPT C2 members*: Component operations staff, user representatives, Component & program office cost estimators, PM, CAE and PEO staff, JCS/J8, OSD (PSA, CAPE (PE), OSD Acquisition Analyst).
- As indicated in Figure 10.9.2.5.5.2.F1, above, IPT C3 is responsible for assessing E1 and E2, forming conclusions thereupon, and recording an explanatory statement that permits the Senior Official to certify "the new estimates of costs, schedule, and performance parameters with respect to the program and system or information technology investment, as applicable, have been determined, with the concurrence of the Director of Cost Assessment and Program Evaluation, to be reasonable." This IPT should:
    - Identify changes that have occurred to the program's requirements.
    - Summarize acquisition and total life-cycle cost growth from the baseline MAR. Display changes in constant (BY) and current (TY) dollars.
    - Include rationale for growth such as technical uncertainties/corrections or changes in inflation, requirements, escalation outlay, quantity, schedule, budget, or estimating errors.
    - Include the assessment (E1) about the "projected cost and schedule for completing the program if current requirements are not modified."
    - Include the assessment (E2) about "projected cost and schedule for completing the program based on reasonable modification of ... requirements."

    - Update the cost estimate and milestone schedule. Note: This portion of the report should contain standard language to explain that these estimates may not be the new baseline, and that when available the revised Original Estimate will be presented in the next MAR.
    - IMPORTANT: The WSARA 2009 requires us to conduct an independent cost analysis in these cases of a MAIS Critical Change if the MDA is USD(AT&L).
    - *IPT C3 members:* Component operations staff, user representatives, Component & program office cost estimators, PM, CAE and PEO staff, JCS/J8, OSD (PSA, CAPE, OSD Acquisition Analyst).
- IPT C4 will document the explanation that permits the Senior Official to certify "the management structure for the program is adequate to manage and control program costs." The IPT C4 should:
    - Review PMO and contractor management structures.
    - Conduct site visits if the IPT Principal Lead determines they would be useful.
    - Re-examine recent program oversight reviews and recommendations to appraise the degree and success of implementation.
    - Develop a draft ADM for the MDA to direct corrective actions.
    - *IPT C4 members*: CAE and PEO staff, PM, OSD (AT&L DDR&E (DT&E, SE) and DPAP, DCIO, OSD Acquisition Analyst).

Table 10.9.2.5.5.3.T1 summarizes recommended IPT membership.

IPT Organization	C1 essential	C2 no alternative	C3 new estimate	C4 management
PMO/PM (as required)	X	X	X	X
PMO Cost/Finance		X	X	
PEO Staff		X	X	X
CAE Staff	X	X	X	X
Component Operations Staff	X	X	X	
User Representatives	X	X	X	
JCS/J8	X	X	X	
OSD Acquisition Analyst	X	X	X	X
DDR&E(DT&E,SE)				X
AT&L(DPAP)				X
OSD CAPE		X	X	
OSD PSA	X	X	X	X
DCIO				X

Table 10.9.2.5.5.3.T1. Summary of Recommended IPT Membership

10.9.2.5.5.4. Critical Change Process Calendar

Figure 10.9.2.5.5.4.F1 portrays a typical Critical Change process calendar and shows the general flow of events described in 10.9.2.5.

Figure 10.9.2.5.5.4.F1. Critical Change Process Calendar

10.9.2.5.5.5. Critical Change Report (CCR)

The Critical Change Report is envisioned to be a document of about six pages: two pages of introduction/background on the program and the events that led to the Critical Change, and one page each for the explanations provided by the IPTs C1-4. The introduction/ background sections should conclude by outlining corrective actions that will be taken to add discipline to program execution and avoid repeated deviation from the new baseline. In most cases an Acquisition Decision Memorandum will also be required to direct the actions cited in the CCR.

In case of an audit, it is important for the Component to keep all records used to prepare the CCR.

10.9.2.5.5.6. Coordination and Transmittal of a CCR to the Congressional Defense Committees

In accordance with the statute (10 U.S.C. 2445c(d)(1)(B)), CCRs must be sent "through the Secretary of Defense, to the congressional defense committees." In cases where the Senior Official is the USD(AT&L), ASD(NII), or DCMO this will be inherent in the CCR coordination and signature process.

In cases where the Senior Official is an SAE, the CCR shall be signed by the SAE (acting as a Senior Official) and provided to an OSD official for transmittal to Congress. The appropriate OSD official is USD(AT&L) (when MDA is retained); the DCMO (when the subject program is a delegated defense business system); or the ASD(NII) (in all other cases). The signed CCR should be provided to the appropriate OSD official with draft Transmittal Letters addressed to the congressional defense committees no later than 5 working days before expiration of the 60-day period.

10.9.2.6. Obligation of Funds

If the Senior Official determines a Critical Change has been reported by a program and a Critical Change Report (CCR) is not submitted to the congressional defense committees within the 60-day period, "appropriated funds may not be obligated for any major contract under the program." For Chapter 144A purposes, the term "major contract" is defined as any contract under the program that is not a firm fixed price contract whose target cost exceeds $17M (FY00 constant dollars); or if no contract exceeds $17M (FY00 constant dollars), then the largest contract under the program.

PMs should not obligate funds for a major contract during the period in which the CCR is being prepared. The prohibition on the obligation of funds will cease to apply on the date on which the congressional defense committees have received a report in compliance with Chapter 144A requirements.

10.9.2.7. Revision of the Original Estimate

Title 10 U.S.C. Chapter 144A permits "an adjustment or revision of the Original Estimate or information originally submitted on a program … if the adjustment or revision is the result of a Critical Change…." Consequently, the determination of a Critical Change and the ensuing program evaluation and delivery of a CCR creates the only opportunity to update the baseline information contained in the MAR.

The urgency with which the CCR is prepared may not allow for the concurrent approval of an updated Acquisition Program Baseline (APB), although the work done to prepare the CCR will be helpful. PMs should make approval of an updated APB before the next MAR cycle a high priority, because the revised original estimate (baseline) in the MAR must be based on a current, MDA-approved APB.

10.9.2.8. Sources for Additional Information

Definitions and the answers to Rarely Asked Questions are provided to clarify issues regarding the NDAA FY07 Section 811 - Time-Certain Development for Department of Defense Information Technology Business Systems; Chapter 144A of title 10 - Major Automated

Information System Programs; and all amendments to Chapter 144A. A complete copy of this Chapter 144A implementation guidance is also available.

10.9.3. MAIS/MDAP Section 817 Determination

Section 817 of the Fiscal Year 2010 National Defense Authorization Act amended Section 2445d of title 10 U.S.C. giving the Secretary of Defense authority to designate a program that meets the definition of a MAIS and an MDAP (referenced herein as MAIS/MDAPs) to be treated as only a MAIS or only as an MDAP.

Section 817 provides that as a general rule:

- A program that requires the development of customized hardware shall be treated only as an MDAP under chapter 144 of title 10 U.S.C., and
- A program that does not require the development of customized hardware shall be treated only as a MAIS program under chapter 144A of title 10 U.S.C.

While these criteria will be employed as a general rule, other factors will also be considered in determining whether to designate a program a MAIS or an MDAP, and will be applied on a case-by-case basis.

10.9.4. Defense Acquisition Executive Summary (DAES)

10.9.4. Defense Acquisition Executive Summary (DAES)

For MDAPs, the DAES is supplemented by the DAES charts (i.e., a monthly 5-slide PowerPoint submission) that provides a *program status, an issues summary, a risk summary, program costs and performance, and an interrelationships, dependencies and synchronization with complementary systems* slide. The program status slide requires specific reporting against cost, schedule, performance, funding and life-cycle sustainment indicators, according to a defined set of criteria for each rating. The quarterly report provides additional programmatic information, to include: mission and description; threshold breaches; program status against defined schedule, performance, and cost parameters; and other information.

For MAIS, the DAES is supplemented by the PM assessment, which is a quarterly submission that may be submitted in PowerPoint, Word or PDF.

The DAES information is designed to provide early-warning reporting to the USD(AT&L) and ASD(NII). The information describes actual program problems, warns of potential program problems, and describes mitigating actions taken or planned. The program manager may obtain permission from USD(AT&L) or ASD(NII) to tailor DAES content. At a minimum, the DAES must report program assessments, unit costs (10 U.S.C. 2433), and current estimates of current APB parameters. It should also report the status of exit criteria.

DAES reporting must present total costs and quantities for all years as projected through the end of the acquisition of the program. In keeping with the concept of total program reporting, the DAES should present best estimates for costs beyond the FYDP, if the FYDP does not otherwise identify those costs. (The total program concept refers to system acquisition activities from Program Initiation through Production and Deployment.)

The Office of USD(AT&L), the Office of ASD(NII), the Offices of DoD CAEs, CIOs, and Program Executive Officers, and the program office should each establish DAES focal points.

10.9.4.1. DAES Reporting

The USD(AT&L) will designate ACAT I programs subject to DAES reporting and assign each program to a quarterly reporting group, for information requiring a quarterly update. (Note: as defined below, some information will require more frequent updates). The ASD(NII) will designate ACAT IA programs subject to DAES reporting and assign each program to a quarterly reporting group. The reporting groups are designated A, B, and C, with Group A reporting in January, April, July, and October, Group B reporting in February, May, August, and November, and Group C in March, June, September, and December.

Program managers will use their Component Acquisition Management Systems (AIM, SMART, and Dashboard) to prepare the quarterly DAES information for electronic transfer via web services to DAMIR by the last working day of the month minus one day for ACAT I programs, and by the last working day of the month for ACAT IA programs. The supplemental DAES charts (for MDAPs) will be prepared using the MS PowerPoint templates, and the PM assessments (for MAIS) will use PowerPoint, Word or PDF until the requirements can be completed online within the Component Acquisition Management systems, at which time future PowerPoint submissions will be eliminated. The slides are currently loaded into DAMIR under Supporting Documentation and can be viewed in Purview within the DAES/Web Services view, in the Supporting Documentation data section. Program Managers should not delay the DAES for any reason.

While most information is required to be updated quarterly to meet statutory and regulatory requirements, other information is required to be updated more frequently or whenever it changes. Table 10.9.3.1.T1 shows the information required and minimum reporting frequency for DAES reporting. Information must be reported at the level of detail required by DAMIR or in accordance with the PowerPoint templates. The data required and level of detail are subject to change as requirements change.

Information	Current Source	Minimum Frequency
Program Information	DAMIR	Annually and within 30 days of a change
Responsible Office	DAMIR	Annually and within 30 days of a change
Mission and Description	DAMIR	Annually and within 30 days of a change
Executive Summary	DAMIR	Monthly
Threshold Breaches	DAMIR	Quarterly
Assessments/Program Status*	DAMIR & PowerPoint Slide	Monthly
Assessments/Program Status (MAIS only)	DAMIR & PowerPoint, Word or PDF slide	Quarterly
Schedule	DAMIR	Quarterly and when program deviation is identified, and with POM/BES submission
Performance	DAMIR	Quarterly and when program deviation is identified
Track to Budget	DAMIR	Annually
Cost and Funding	DAMIR	Quarterly and when program deviation is identified, and with POM/BES submission
Unit Cost*	DAMIR	Quarterly
Contracts and Earned Value	DAMIR	Monthly
Deliveries and Expenditures	DAMIR	Quarterly
Operating and Support Costs	DAMIR	Quarterly
Issues Summary*	PowerPoint/DAMIR	Monthly
Risk Summary*	PowerPoint/DAMIR	Monthly
Program Costs and Performance*	PowerPoint/DAMIR	Monthly
Interrelationships and	PowerPoint/DAMIR	Monthly

Dependencies*		

* MDAP Only

Table 10.9.4.1.T1. DAES/Web Services Information Requirements

10.9.4.2. POM/BES Submissions

Within 30 days of the POM/BES, the program manager shall submit a POM/BES DAES using DAMIR that at a minimum includes POM/BES cost and funding, schedule, and unit cost. The POM DAES is submitted in even years, and the BES DAES is submitted in odd years.

10.9.4.3. Consistency of DAES Information

DAES information should be consistent with the information in the latest ADM, APB, and other mandatory or approved program documentation. Information such as Program Manager and Points of Contact should be updated and pushed via web services to DAMIR with the regular monthly updates.

10.9.5. Defense Acquisition Management Information Retrieval (DAMIR)

10.9.5. Defense Acquisition Management Information Retrieval (DAMIR)

The Defense Acquisition Management Information Retrieval (DAMIR) creates a net-centric environment to provide data transparency of acquisition management information to the Department. DAMIR provides: full web-services data exchange with Components' Acquisition Information Systems for DAES information; SAR and APB Web applications that allow Components to input SAR and APB data, making DAMIR the authoritative source for this information; analytical tools that enable users to customize the way they search, view, and display previously unavailable combinations of information electronically; and workflow and collaboration capabilities.

Based upon an OSD enterprise decision, the use of DAMIR is mandatory for all MDAPs and MAIS acquisition programs and must be employed to satisfy statutory requirements for SAR submission. Non-MDAP and non-MAIS programs may also use the system.

The Director, Acquisition Resources and Analysis, has responsibility for the development, upgrade, and maintenance of DAMIR. User help can be obtained through the following sources:

- DAMIR public web site (www.acq.osd.mil/damir)
- DAMIR hotline (703-679-5345)
- DAMIR mailboxes (cars@caci.com or damir@osd.mil)

10.9.5.1. DAMIR APBs

All APBs for ACAT I and IA programs must be created and released using DAMIR. DAMIR provides the data entry capability and required workflow to create and edit an APB. Once an APB is approved and released, it can no longer be edited. The APB Objectives and Thresholds will also be visible within both the SAR and DAES.

10.9.5.2. DAMIR SARs

As DAMIR is the authoritative source for SARs, DAMIR provides the data entry capability and required workflow to create and edit a SAR. The computational model capability, previously found in CARS, is also integrated into the SAR module of DAMIR. DAMIR provides extensive data checks, ensuring that a SAR is not released to Congress with critical errors. APB values are pulled from the APB module and can not be edited within the SAR. All MDAP programs are required to use DAMIR to prepare the annual and quarterly SARs. Hard copy SARs are no longer submitted to Congress. Instead, Congress is granted access to the SAR information through DAMIR.

10.9.5.3. DAMIR DAES

To improve information sharing and to reduce duplicate data entry, DAES information is now obtained via web services data exchange between the Components' Acquisition Information Systems and DAMIR. All ACAT I and IA programs are required to submit their information to a Component Acquisition Information System that has the capability to exchange information with DAMIR in a prescribed format. APB values displayed in the DAES are pulled from the APB module and cannot be updated via web services.

Assessments/Program Status is the only DAES section where the Program Manager has the option of directly entering the information into DAMIR or submitting it via web services. If Assessments are not being submitted monthly via web services, then they must be entered into DAMIR.

Access to DAES information is based on permissions.

10.9.5.4. DAMIR Ad Hoc Reports

DAMIR Ad Hoc reports provide analytical capability and cross-program analysis. Access to reports is permission based, but all users have access to SARs and SAR Ad Hoc reports.

The Director, Acquisition Resources and Analysis, has responsibility for the development, upgrade, and maintenance of DAMIR. Direct questions and requests for copies of the software should be directed to that organization. The DAMIR software includes instructions for preparing the APB, SAR, DAES, and UCR, including administrative procedures. The DAMIR web page also has the instructions and a DAMIR "help line" is available as well.

10.10. Special Interest Programs

10.10. Special Interest Programs

A program, or a technology project that will result in a program, has special interest if it has one or more of the following factors: technological complexity; Congressional interest; a large commitment of resources; the program is critical to achievement of a capability or set of capabilities; the program is part of a system of systems; or the program is a joint program. Generally, the level of funding, desired oversight and reporting will determine the MDA and whether or not the program is designated a "Special Interest" program. Programs that already meet the dollar thresholds for an MDAP, Major System, or MAIS program cannot also be designated Special Interest programs.

10.10.1. MDAP or Special Interest Programs

If a program meets one of the dollar thresholds for it to be designated an MDAP, then the program is an MDAP. If the program is below the dollar threshold for designation as an MDAP, the DAE may still designate the program an MDAP if the DAE deems oversight with statutory reporting is needed. An MDAP is designated ACAT I and its oversight comes from the DAE. The DAE can either retain MDA or delegate it to a Component Head or CAE. If the DAE retains MDA, the program is an ACAT ID program. If the DAE delegates MDA to the Component Head or CAE, then the program is an ACAT IC program. As an MDAP, the program must meet all statutory reporting requirements for MDAP programs.

If the DAE desires oversight of a program that falls below MDAP dollar thresholds, and deems that statutory reporting associated with MDAPs is not needed, the program is designated a

Special Interest Program. If the DAE retains MDA, the program is an ACAT ID Special Interest program. If the DAE delegates MDA to the Component Head or CAE, then the program is an ACAT IC Special Interest program. The CAE may also designate Special Interest programs that are ACAT II or below. For such Special Interest programs, the reporting requirements are tailored to meet the specific oversight needs.

10.10.2. MAIS or Special Interest Programs

If an Automated Information System (AIS) program meets one of the dollar thresholds for it to be designated a MAIS, then the program is a MAIS program. If the program falls below the MAIS dollar thresholds, the MDA may still designate the program a MAIS program if the MDA deems that oversight with statutory reporting is needed. A MAIS program is designated ACAT IA and the MDA is the DAE or the person within OSD to whom MDA has been delegated. If the MDA remains within OSD (DAE or delegated MDA within OSD), the program is an ACAT IAM. If MDA is delegated to the Component Head or CAE, then the program is an ACAT IAC. A MAIS program must meet all statutory reporting requirements for MAIS programs.

If the DAE (or delegated MDA within OSD) desires oversight of an AIS program, but deems that the statutory reporting associated with MAIS programs is not needed, the program is designated a "Special Interest" program. If MDA remains within OSD (DAE or DAE delegated MDA within OSD), the program is an ACAT IAM Special Interest program. If MDA is delegated by the DAE to the Component Head or CAE, then the program is an ACAT IAC Special Interest program.

For such Special Interest programs, the reporting requirements are tailored to meet the specific oversight needs.

DEFENSE ACQUISITION GUIDEBOOK
Chapter 11 -- Program Management Activities

11.0. Overview

11.0.1. Purpose

The purpose of this chapter is to describe and explain some of the activities and decisions available to and required of the program manager as he or she manages and executes the program.

11.0.2. Contents

Chapter 11 covers the following topics:

Additional information regarding Program Management can be found at the DAU Acquisition Community Connection website, the Program Management Community of Practice.

11.1. Joint Programs

11.1. Joint Programs

There are two aspects of "jointness" to consider when discussing joint program management: the jointness of the capability and the jointness of the development and production of the system.

11.1.1. Identifying Joint Capabilities

As part of the Joint Capabilities Integration and Development System (JCIDS), the Joint Staff J-8, with the assistance of the DoD Components, evaluates all JCIDS documents, regardless of Acquisition Category or previous delegation decisions or Joint Potential Designation decisions, to determine whether the proposal has joint force implications. The Joint Staff documents, CJCS Instruction 3170.01 and the JCIDS Manual, provide full detail and direction on this topic.

11.1.2. Joint Acquisition Management

Acquisitions that contribute to joint capabilities may be managed as joint acquisition programs. A "joint acquisition" is any acquisition system, subsystem, component, or technology program with a strategy that includes funding by more than one DoD Component during any phase of a system's life cycle. DoD Instruction 5000.02, Enclosure 10, paragraph 4 addresses DoD Component fiscal responsibilities associated with participation in programs under joint acquisition management.

11.1.2.1. Designation

Considering the assigned Joint Potential Designator and the recommendation of the Heads of the DoD Components, the Milestone Decision Authority decides whether to place the program under joint acquisition management. The Milestone Decision Authority should make this decision and, if appropriate, designate the Lead Executive DoD Component, as early as possible in the acquisition process.

The DoD Components should periodically review their programs to determine the potential for joint cooperation. The DoD Components should structure program strategies to encourage and to provide an opportunity for multi-Component participation.

11.1.2.2. Execution

The designated Lead Executive DoD Component for a joint acquisition should act on behalf of all DoD Components involved in the acquisition.

A Memorandum of Agreement should specify the relationship and respective responsibilities of the Lead Executive DoD Component and the other participating components. The Memorandum of Agreement should address system capabilities and the development of capabilities documents, funding, manpower, and the approval process for other program documentation.

The following additional considerations have proven effective in managing joint programs:

- The assignment of a Lead Executive DoD Component should consider the demonstrated best business practices of the DoD Components, including plans for effective, economical, and efficient management of the joint program; and the demonstrated willingness of the DoD Component to fund the core program, essential to meeting joint program needs.
- The Milestone Decision Authority and DoD Components should consolidate and co-locate the supporting efforts of the joint program at the Lead Executive DoD Component's program office, to the maximum extent practicable.
- The Component Acquisition Executive of the Lead Executive DoD Component should optimally use the acquisition organizations, test organizations, and other facilities of all Military Departments.
- The designated Lead Executive DoD Component selects the qualified program manager for the designated program under joint acquisition. The single program manager should then be fully responsible and accountable for the cost, schedule, and performance of the development system.
- If the joint program results from a consolidation of several different DoD Component programs, each with a separate program manager, the selected joint program manager should have the necessary responsibility and authority to effectively manage the overall system development and integration.
- A designated program under joint acquisition should have one quality assurance program, one program change control program, one integrated test program, and one set of documentation and reports (specifically: one set of capabilities documents, (with Service unique capability requirements identified), one Information Support Plan, one Test and Evaluation Master Plan, one Acquisition Program Baseline, etc.).
- The Milestone Decision Authority should designate the lead Operational Test Agency to coordinate all operational test and evaluation. The lead Operational Test Agency should produce a single operational effectiveness and suitability report for the program.
- Documentation for decision points and periodic reporting should flow only through the Lead Executive DoD Component acquisition chain, supported by the participating components.
- The program should use inter-DoD Component logistics support to the maximum extent practicable, consistent with effective support to the operational forces and efficient use of DoD resources.
- Unless statute, the Milestone Decision Authority, or a memorandum of agreement signed by all DoD Components directs otherwise, the Lead Executive DoD Component should budget for and manage the common Research, Development, Test, and Evaluation funds for the assigned joint programs.
- Individual DoD Components should budget for their unique requirements.

11.2. Considerations for International Cooperation

11.2.1. International Cooperative Programs

11.2.1. International Cooperative Programs

An international cooperative program is any acquisition program or technology project that includes participation by one or more foreign nations, through an international agreement, during any phase of a system's life cycle. The key objectives of international cooperative programs are to reduce weapons system acquisition costs through cooperative development, production, and support; and to enhance interoperability with coalition partners.

11.2.1.1. International Considerations and Program Strategy

Title 10 U.S.C. 2350a(e) as amended by Section 1251 of the National Defense Authorization Act for Fiscal Year 2008 requires an analysis of potential opportunities for international cooperation for all Acquisition Category I programs before the first milestone or decision point. DoD Directive 5000.01, Enclosure 1, and DoD Instruction 5000.02, Enclosure 10, paragraph 5, specify the requirements for international considerations; amplifying guidance and information appears in this Guidebook. DoD Directive 5000.01 requires International Armaments Cooperation; requires interoperability with U.S. coalition partners; and establishes the preference for a cooperative development program with one or more Allied nations over a new, joint, or DoD Component-unique development program.

During the development of the Technology Development Strategy (TDS) for Milestone A or the initial Acquisition Strategy for Milestone B for a new program, the potential for international cooperative research, development, production, and logistic support should be addressed, and thereafter, the potential for international cooperation should be considered in every phase of the acquisition process. DoD Components should periodically review their programs to determine the potential for international cooperation. Milestone Decision Authorities may recommend forming international cooperative programs based on the TDS or acquisition strategy considerations; DoD Component Heads may also recommend forming international cooperative programs. The Milestone Decision Authority should make the decision to establish an international cooperative program as early as possible in the Defense Acquisition Management System.

The Milestone Decision Authority, with the advice and counsel of the DoD Components and the Joint Requirements Oversight Council, makes the decision to pursue an international cooperative program. The decision process should consider the following:

- Demonstrated best business practices, including a plan for effective, economical, and efficient management of the international cooperative program;
- Demonstrated DoD Component willingness to fully fund their share of international cooperative program needs;
- The long-term interoperability and political-military benefits that may accrue from international cooperation; and
- The international program's management structure as documented in the international agreement. The designated program manager (U.S. or foreign) is fully responsible and accountable for the cost, schedule, and performance of the resulting system.

The DoD Component remains responsible for preparation and approval of most statutory, regulatory, and contracting reports and milestone requirements, as listed in DoD Instruction 5000.02, Enclosure 4. Documentation for decision reviews and periodic reports flow through the DoD Component acquisition chain, supported by the participating nation(s).

International cooperation can add stability to the program. DoD Instruction 5000.02 prevents DoD Components from terminating or substantially reducing participation in international cooperative programs under signed international agreements without Milestone Decision Authority notification, and in some cases, Milestone Decision Authority approval.

Additional information may be found in the Director, International Cooperation, International Armaments Cooperation Handbook.

11.2.1.2. International Considerations within the Acquisition Management Framework

Establishing and maintaining cooperative relationships with friends and Allies are critical to achieving interoperability of equipment and services to

> *be used by the U.S. Armed Forces and our coalition partners; to achieving access to technology from sources worldwide; to achieving economies of scale with our investment resources; and to expanding our influence in critical areas of the world* (USD(AT&L) Memorandum, Support for International Armaments Cooperation Activities, January 23, 2006)

International programs may be established at any point in the defense acquisition management system when justified as a prudent business judgment. Figure 11.2.1.2.F1 depicts the key considerations for each phase:

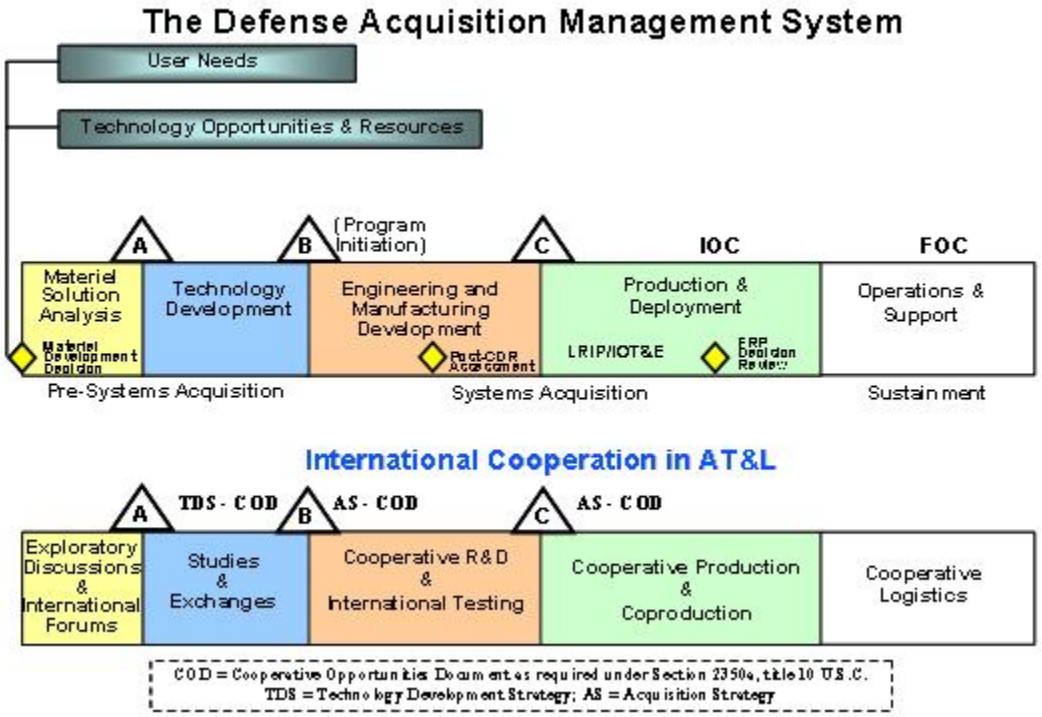


Figure 11.2.1.2.F1. Key International Cooperative considerations during Acquisition.

Determination of User Needs & Exploring Technology Opportunities (Early Technology Projects). The efforts needed to identify cooperative development opportunities before entering into a formal acquisition program are often challenging, but such activities capitalize on high payoffs in cost savings and interoperability when successful. Formulation of cooperative development programs involves resolution of issues in the areas of requirements harmonization, cost sharing, work sharing, technology transfer, intellectual property rights, and many others. While multinational force compatibility may increase system acquisition cost, it can provide more cost-effective defense for the whole force through increased interoperability and reduced life-cycle costs. Cooperative opportunities identification and formulation should be pursued during the earliest stages of the pre-systems acquisition research and development process to

maximize the chance for success. DoD Instruction 5000.02, Enclosure 3, paragraph 2, identifies technology projects and initiatives.

Using the Joint Capabilities Integration and Development System process, representatives from multiple DoD communities formulate broad, time-phased, operational goals, and describe requisite capabilities in the Initial Capabilities Document. They examine multiple concepts and materiel approaches to optimize the way the Department of Defense provides these capabilities. This examination includes robust analyses that consider affordability, technology maturity, and responsiveness.

Several important mechanisms available to provide insight into the needs of potential foreign partners are exploratory discussions, international forums, studies, and the exchanges of information and personnel:

Exploratory Discussions. Before entering into an international project, many forms of dialogue can take place with potential partners. These informal discussions are usually called exploratory discussions or technical discussions--they are NOT called "negotiations," which requires a legal authority and formal permission from the Office of the Secretary of Defense. The avoidance of any binding commitments on the part of the U.S. Government, and the absence of any draft, international agreements characterize exploratory discussions. Other than the two exclusions above, the parties may discuss most other topics, provided release authority has been obtained for any information provided by DoD representatives or defense contractors.

International Forums. There are many international forums dedicated to discussing mutual armaments needs and early technology projects. These forums include the Conference of National Armaments Directors (CNAD), whose U.S. representative is the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)). The CNAD's subsidiaries are the "Main Armaments Groups," particularly the NATO Army Armaments Group, NATO Navy Armaments Group, and the NATO Air Force Armaments Group. The NATO Research and Technology Organization conducts and promotes cooperative research and information exchange in NATO. The Technical Cooperation Program with Australia, Canada, New Zealand, and the United Kingdom is another multilateral forum dedicated to cooperation in conventional military technology development. In addition there are about 30 bilateral forums, such as the U.S.-Japan Systems and Technology Forum and the U.S./Canadian Armaments Cooperation Management Committee, that have a similar purpose.

Studies. It is normal for the DoD and potential partners to conduct studies before entering into a cooperative acquisition project. These studies can be conducted years before the project starts, and are often called feasibility studies, or pre-feasibility studies. Industry, government agencies, or a combination of both generally conduct the feasibility studies, with the objective of providing a technical appraisal of the feasibility of developing and producing equipment. These studies can develop input for the Analysis of Alternatives required by DoD before the start of a new acquisition program.

International Exchanges of Information and Personnel. A common source for cooperative program opportunity identification is the Defense Research, Development, Test and Evaluation Information Exchange Program (IEP), which provides a standardized way of conducting bilateral science and technology information exchange (formerly called data exchange). The IEP has proven extremely useful as a means of cooperative opportunities formulation. Another source for identifying cooperative opportunities is the Defense Personnel Exchange Program, especially the Engineer and Scientist Exchange Program (ESEP).

Pre-Systems Acquisition. Decisions made during the Materiel Solution Analysis and Technology Development phases of Pre-Systems Acquisition generally define the nature of the entire program. Once the program enters the Engineering and Manufacturing Development phase, it is difficult to adopt major changes without significant schedule or cost adjustments. Consequently, the decision to include international partners needs to be addressed as early as possible, preferably during development of the Initial Capabilities Document, but no later than during the Materiel Solution Analysis phase.

To meet the requirements of Title 10 U.S.C. 2350a(e), the Technology Development Strategy prepared for Milestone A or the Acquisition Strategyfor Milestones B and C must address the following areas:

a. Is a similar project in development or production by NATO, a NATO organization, a member nation of NATO, a major non-NATO ally, or friendly foreign country?
b. If so, then the Technology Development Strategy or initial acquisition strategy must provide an assessment of that project as to whether or not it could satisfy or be modified to satisfy U.S. military requirements, and
c. An assessment of the advantages and disadvantages with regard to program timing, developmental and life-cycle costs, technology sharing, and Rationalization, Standardization, Interoperability of a cooperative development program.
d. The USD(AT&L) provides a recommendation whether or not the feasibility and desirability of a cooperative development program should be explored.
e. What alternate forms of cooperation could be appropriate for the project?

Except for e) above, these considerations are based on 10 U.S.C. 2350a requirements. They force the consideration of alternative forms of international cooperation. Even if cooperative development is impractical, cooperative production, foreign military sales, licensed production, component/subcomponent co-development, or incorporation of subsystems from allied or friendly foreign sources should be considered and may be appropriate.

DoD Components should fully investigate potential cooperative opportunities as part of the Technology Development Strategy and acquisition strategy development. Program proponents should consult with the appropriate international programs organization to obtain assistance in addressing international considerations during Technology Development Strategy or acquisition strategy development for programs in all acquisition categories.

Engineering and Manufacturing Development. After program initiation, during Engineering and Manufacturing Development, key elements of the system design are defined, and system/subsystem development begins. Major changes often present schedule delays that program managers are unwilling to accept; however, there have been numerous examples of successful subsystem cooperative development partnerships that have been formed during the Engineering and Manufacturing Development Phase. Once a program has reached this phase, absent cooperation in earlier stages, there will be only limited opportunity to bring other nations on as full cooperative development partners. Consequently, if the opportunity for cooperation in subsystem development arises prior to or during Engineering and Manufacturing Development, consult with the appropriate international programs organization to obtain further assistance.

Foreign Comparative Testing. A viable alternative to development is the acquisition of commercial items. While individual acquisition programs can conduct evaluations with their own resources, the Foreign Comparative Testing Program offers a structured and funded means for program offices to evaluate the suitability of a foreign developed item for purchase in lieu of developing a similar U.S. item.

International Test Operations Procedures. The International Test Operations Procedures (ITOP) program provides for international agreements that document state-of-the-art test techniques for technical testing of military material and allows the exchange of test data to avoid redundant testing when foreign equipment is purchased. Currently there are over 130 ITOPs with Germany, France, and the UK covering a variety of test types and/or equipment class. Through ITOPs, the U.S. has access to latest test technology and procedures of our allies, which could possibly be utilized by DoD program managers. The ITOP program is managed at OSD by the Office of the Director, Operational Test and Evaluation.

Production and Deployment Phase. There are three basic mechanisms for transfer of U.S. produced defense articles and associated production capability to other nations: sales, co-production and cooperative production. Sales under the Foreign Military Sales Program foreign co-production of a U.S. developed system, fall under the purview of the Defense Security Cooperation Agency (DSCA). The Department of State is responsible for transfer of defense articles and associated production capability under export licenses. Both DSCA and the Defense Technology Security Administration coordinate closely with the responsible DoD Component regarding the development and implementation of DoD co-production policy in their respective areas of responsibility. USD(AT&L) is responsible for oversight of the third basic mechanism, cooperative production. Cooperative production is a joint or concurrent international production arrangement arising from a cooperative development project. Examples of this type of production program are the Rolling Airframe Missile and the Multi-Functional Information Distribution System. Cooperative production falls under the authority of the Arms Export Control Act Section 2751.

Operations & Support Phase. Cooperative logistics refers to cooperation between the U.S. and allied or friendly nations or international organizations in the logistical support of defense systems and equipment. Cooperative logistics is part of the acquisition process, but as a

substantial part of military operations, much of the implementation process involves Security Assistance processes and procedures.

Cooperative logistics support includes:

- Logistics Cooperation international agreements (IAs), used to improve sharing of logistics support information and standards, and to monitor accomplishment of specific cooperative logistics programs;
- Acquisition and Cross-Servicing Agreements;
- Host Nation Support;
- Cooperative Logistics Supply Support Arrangements;
- Cooperative Military Airlift Agreements;
- War Reserve Stocks for Allies;
- Agreements for acceptance and use of real property or services;
- Standardization of procedures under American/British/Canadian/Australian/New Zealand auspices;
- International Standardization Agreements developed in conjunction with member nations of the North Atlantic Treaty Organization and other allies and coalition partners, as described in DoD 4120.24-M, "Defense Standardization Program (DSP) Policies and Procedures" and as listed in the Acquisition Streamlining and Standardization Information System (ASSIST) database (login required);
- Consideration of the interoperability implications of these agreements when constructing Work Breakdown Structures; and
- Planning support provided by the Program Manager's Tool (login required).

Each participant or party involved in cooperative logistics agreements should benefit from the agreement. Benefits could be tangible, such as the U.S. receiving support for its naval vessels when in a foreign port; or intangible, such as the foreign nation receiving the implied benefit of a visible, U.S. naval presence in the region. Other cases are more obviously quid-pro-quo: cross-servicing agreements, for example. In a cross-servicing agreement, each party receives the equivalent of the materiel or services provided to the other party. Besides the obvious material benefits, such agreements have the collateral effects of opening dialog and creating relationships between the parties. Such dialog and relationships may serve to strengthen political bonds. While not a program manager responsibility, DoD acquisition personnel should be aware of the international consequences of their activities and appropriately support such efforts.

11.2.1.3. International Cooperative Program Protection

Program protection considerations play a major role in international cooperative programs for obvious reasons. The program manager should consider technology security factors when developing an international cooperative program. The Defense Technology Security Administration, in concert with DoD Component technology security organizations, is the focal point within the DoD for technology security. Program managers should contact their DoD

Component technology security organization early enough in the process to ensure that technology security factors that may affect cooperative efforts are taken into consideration.

The program manager should consider technology release in the initial planning of an international cooperative program through a review of National Disclosure Policy foreign disclosure guidance and development of the foreign disclosure and export control elements of the program's Technology Assessment/Control Plan . Early consideration of National Disclosure Policy requirements and foreign disclosure/export control planning in an international cooperative program should enable the international program to avoid major cost, schedule, and performance goal impacts.

DoD Instruction 5000.02, Enclosure 10, paragraph 5, and the tables of enclosure 4 establish international cooperative program protection policy requirements. Chapter 8 of this Guidebook provides additional insights into this policy.

11.2.1.3.1. Classification Guide

In addition to the Program Protection Plan required by all programs containing Critical Program Information, and the Technology Assessment/Control Plan, DoD 5200.1-R requires international programs to develop a classification guide for all programs containing classified information of either party. The classification guide, as prescribed in DoD Directive 5230.11, identifies the items or information to be protected in the program, and indicates the specific classification to be assigned to each item.

11.2.1.3.2. Program Security Instruction (PSI)

A PSI details security arrangements for the program and harmonizes the requirements of the participants' national laws and regulations. Using the Under Secretary of Defense for Acquisition, Technology and Logistics international agreements streamlined procedures authorized by DoD Instruction 5000.02, Enclosure 10, paragraph 5, the International Agreements Generator will lead the program manager through the considerations for, and the development of, a PSI. Additional information about the PSI is found in the International Armaments Cooperation Handbook.

If all security arrangements to be used in an international program are in accordance with an existing industrial security arrangement between the participants, a separate PSI is not required.

11.2.1.3.3. Delegation of Disclosure Authority Letter (DDL)

Per DoD Instruction 5000.02, a written authorization to disclose any classified or controlled unclassified information must be obtained prior to entering discussions with potential foreign partners. The authorization for release of classified information (developed or used during any part of the life cycle of the program) to any potential or actual foreign participants in the program

will be in the form of a Delegation of Disclosure Authority Letter (DDL), as prescribed in DoD Directive 5230.11, or other written authorization issued by the DoD Component Foreign Disclosure Office. The authorization for release of classified or controlled unclassified information must comply with DoD Component policies for release of such information.

11.2.1.3.4. Technology Release Roadmap (TRR)

Prior to the Engineering and Manufacturing Development phase of an acquisition program with substantial international involvement by foreign industry, the program manager should prepare an export control TRR as part of their Technology Assessment/Control Plan (TA/CP). This TRR will provide a projection of when export licenses will be required in support of the acquisition process, and when critical milestones regarding national disclosure policy implementation will need to be addressed. The TRR must be consistent with the program's TA/CP, Security Classification Guide (SCG), and other disclosure guidance.

The TRR accomplishes the following:

- Provides early DoD Component planning for the program's proposed technology releases to foreign industry consistent with the National Disclosure Policy.
- Provides early planning for higher-level (i.e., above DoD Component-level) special technical reviews and approvals (i.e. Low Observable/Counter Low Observable, anti-tamper, cryptography) needed in support of proposed technology releases to foreign industry.
- Establishes a detailed export license approval planning process for U.S.-foreign industry cooperation to meet critical program and contract timelines.

The TRR includes three sections: 1) A timeline mapping key projected export licenses against the program acquisition schedule; 2) A definition of the technologies involved in each export license; and 3) A list of U.S. contractors (exporters) as well as foreign contractors (end users) for each license.

11.2.2. Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L))-Related International Agreement Procedures

11.2.2. Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L))-Related International Agreement Procedures

An International Agreement (IA) is any agreement concluded with one or more foreign governments including their agencies, instrumentalities, or political subdivisions, or with an international organization. The IA delineates respective responsibilities and is binding under international law. IAs are required by U.S. law for all international cooperative projects.

Per DoD Instruction 5000.02 , all AT&L-related international agreements may use the USD(AT&L)-issued streamlined procedures found in this Guidebook and in the International Armaments Cooperation Handbook, rather than following the lengthy documentation requirements mandated by DoD Directive 5530.3, "International Agreements."

11.2.2.1. Preparation and Documentation

The following considerations apply to the preparation of and documentation associated with Acquisition, Technology and Logistics-related international agreements:

- Program managers or project leaders consult with the DoD Component's international programs organization, as well as foreign disclosure, legal, and comptroller personnel, to develop international agreements.
- The DoD Components develop international agreements in accordance with the provisions of the most recent version of DoD International Agreement Generator computer software.
- Prior to initiating formal international agreement negotiations, the DoD Components prepare a Request for Authority to Develop and Negotiate (RAD) that consists of a cover document requesting such authority and a Summary Statement of Intent (SSOI) that describes the DoD Component's proposed approach to negotiations. DoD Components that have not been delegated authority to negotiate (currently the three Military Departments and the Missile Defense Agency have such authority) normally are required to provide a copy of the draft international agreement prior to RAD approval.
- Prior to signing an international agreement, the DoD Components prepare a Request for Final Approval (RFA) that consists of a cover document requesting such authority, a revised SSOI that describes the outcome of negotiations, and the full text of the international agreement to be signed on behalf of the Department of Defense.
- The DoD Components should use the Streamlining I Coordination Process for both the RAD and the RFA. They should apply to Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L))/International Cooperation to be

delegated authority to use Streamlining II procedures for processing International Agreements. If Streamlining II authority is or has been delegated, the DoD Component should use the streamlined process. (To date, the Office of the USD(AT&L)/International Cooperation has only delegated Streamlining II authority to the Department of the Navy.)

11.2.2.2. Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (OUSD(AT&L)) Oversight

OUSD(AT&L)/International Cooperation provides the following international agreement oversight support:

- Approves and makes available the following agreement process guidance:
  - Request for Authority to Develop (RAD);
  - Request for Final Approval (RFA);
  - Summary Statement of Intent (SSOI);
  - Arms Export Control Act Section 27 Project Certification format requirements; and
  - DoD International Agreement Generator computer software.
- Approves the following agreement process actions:
  - RADs and RFAs for Memoranda of Understanding (MOU)/Memoranda of Agreement (MOA);
  - Project Agreements and Arrangements;
  - Arms Export Control Act Section 65 Loan Agreements;
  - End-User Certificate (EUC) Waivers;
  - The Foreign Military Sales of items which have not completed operational test and evaluation successfully (Yockey Waivers); and
  - DoD Component requests for DoD International Agreement Generator text deviations or waivers requested in RAD and RFA submissions.
- Delegates PA negotiation authority under the Streamlining I Coordination (Approval) Process to specifically designated DoD Components.
- Certifies DoD Component international agreement processes to the Streamlining II standards prior to delegation of RAD/RFA authority to a DoD Component.
- Decertifies a DoD Component international agreement process in the event minimum quality standards are not maintained.
- Resolves RAD/RFA coordination process disputes.
- Supports satisfaction of the following statutory requirements:
  - Obtains USD(AT&L) determination under 10 U.S.C. 2350a paragraph (b) for all international agreements that rely upon this statute as their legal authority;
  - Notifies Congress of all Arms Export Control Act Section 27 (see 22 U.S.C. Section 2767, "Authority of President to enter into cooperative projects with friendly foreign countries") international agreements a minimum of 30 calendar days prior to authorizing agreement signature; and

- Conducts interagency coordination with the Department of State, Department of Commerce, and the Department of the Treasury (see 22 U.S.C. 2767 and DoD Directive 5530.3).

11.2.2.3. Coordination Processes

There are two accredited international agreement coordination processes: Streamlining I and Streamlining II .

11.2.2.3.1. International Agreement Streamlining I Process

Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L))/International Cooperation (IC) uses the following Streamlining I process unless it has delegated coordination authority to the DoD Component:

- **Request for Authority to Develop and Negotiate (RAD) Memorandum of Understanding (MOUs) and Memorandum of Agreements (MOAs)**. The DoD Component prepares the RAD and obtains OUSD(AT&L)/IC approval prior to initiating MOU or MOA negotiations. If applicable, the DoD Component develops and submits Coalition Warfare Program (CWP) funding requests associated with the RAD, in accordance with the CWP Management Plan. OUSD(AT&L)/IC conducts DoD and interagency coordination, as appropriate, using a standard review period of 21 working days, which may expedited at OUSD(AT&L)/IC's discretion.
- **RAD Program Authorizations (PAs) and Section 65 Loan Agreements**. Unless OUSD(AT&L)/IC delegates PA negotiation authority, the DoD Component prepares a RAD and obtains OUSD(AT&L)/IC approval prior to initiating PA or Section 65 Loan Agreement negotiations. OUSD(AT&L)/IC conducts interagency coordination, as appropriate, using a standard review period of 15 working days, which may be expedited at OUSD(AT&L)/IC's discretion.
- **Negotiation**. Generally, within 9 months of receipt of RAD authority, the DoD Component negotiates the international agreement in accordance with the provisions of the most recent version of DoD International Agreement Generator.
- **Request for Final Approval to Conclude (RFA) MOUs and MOAs**. The DoD Component prepares the RFA and obtains OUSD(AT&L)/IC approval prior to signing the MOU or MOA. RFAs for agreements relying upon Arms Export Control Act (AECA) Section 27 as the legal authority for the international agreement will also include a Project Certification. OUSD(AT&L)/IC conducts interagency coordination, as appropriate, based upon a standard review period of 21 working days, which may be expedited at OUSD(AT&L)/IC's discretion. OUSD(AT&L)/IC provides Congress with any required AECA Section 27 notifications.
- **RFA PAs and Section 65 Loan Agreements**. The DoD Component submits RFAs notifying OUSD(AT&L)/IC of its intention to sign PAs and Section 65 Loan Agreements prior to concluding such agreements. AT&L/IC conducts interagency coordination, as

appropriate, based upon a review period of 15 working days, which may be expedited at OUSD(AT&L)/IC's discretion. OUSD(AT&L)/IC provides Congress with any required AECA Section 27 notifications.

11.2.2.3.2. International Agreement Streamlining II Process

Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L))/International Cooperation (IC) may delegate approval authority for the Request for Authority to Develop and Negotiate/Request for Final Approval (RAD/RFA) for all international agreements associated with programs with a total program value of less than $25M (in FY01 constant dollars) and for Acquisition Category II and Acquisition Category III programs to the DoD Component Acquisition Executive. The DoD Component Acquisition Executive may subsequently re-delegate RAD/RFA authority for programs with a total program value of less that $10M (in FY01 constant dollars) and Acquisition Category III programs to the Head of the DoD Component's international programs organization. The following procedures will apply:

- The DoD Components will obtain the concurrence of their legal, financial management, and foreign disclosure organizations prior to approving RADs/RFAs.
- The DoD Components will forward coordination disputes to OUSD(AT&L)/IC for resolution.
- The DoD Components will send Notices of Intent to Negotiate (NINs) or Notices of Intent to Conclude (NICs) to OUSD(AT&L)/IC for all approved RADs and RFAs. NINs will include the DoD Component's approval document and program Summary Statement of Intent. NICs will also include the final international agreement text to be signed, plus an Arms Export Control Act Section 27 Project Certification, if required. The DoD Components will not sign international agreements until a 15-working-day period (for PAs and Loans) or 21-working-day period (for Memoranda of Understanding) after AT&L/IC receipt of the NIC has elapsed and any required 10 U.S.C. 2350a approval or AECA Section 27 Congressional notification process has been completed.
- OUSD(AT&L/IC) may, at its discretion, decide to waive these rules on a case-by-case basis and require that certain agreements receive specific OUSD(AT&L/IC) approval before conclusion.
- OUSD(AT&L)/IC will use NINs, NICs and other relevant information to verify DoD Component international agreement process quality.
- Generally, within 9 months of receipt of RAD authority, DoD Component personnel will negotiate the international agreement in accordance with the provisions of the most recent version of DoD International Agreement Generator.

11.2.2.3.3. Coordination of Requests for Authority to Develop and Negotiate (RADs), Requests for Final Approval (RFAs), Notices of Intent to Negotiate (NINs), and Notices of Intent to Conclude (NICs) Relating to Nuclear, Chemical, and Biological (NCB) Fields

The Office of the Under Secretary of Defense for Acquisition, Technology and Logistics/International Cooperation coordinates all international agreements (including Memoranda of Understanding, Project Arrangements, other similar agreements) and Information Exchange Program annexes relating to NCB warfare technologies (including defenses against such technologies) with the Assistant to the Secretary of Defense (Nuclear and Chemical and Biological Defense Programs) prior to approving the agreement. DoD policy requires this coordination for NCB-related RADs for project arrangements under Streamlining I authority, and for NINs and NICs under Streamlining II authority.

11.2.3. Acquisition and Cross-Servicing Agreements (ACSAs)

11.2.3. Acquisition and Cross-Servicing Agreements (ACSAs)

ACSAs are bilateral international agreements that allow for the provision of cooperative logistics support under the authority granted in 10 U.S.C. Sections 2341-2350. They are governed by DoD Directive 2010.9, "Acquisition and Cross-Servicing Agreements" and implemented by CJCS Instruction 2120.01, "Acquisition and Cross-Servicing Agreements." ACSAs are intended to provide an alternative acquisition option for logistics support in support of exercises or exigencies.

11.2.3.1. Types of Acquisition and Cross-Servicing Agreements (ACSAs) Authorities

Title 10 of the United States Code provides two legal authorities for foreign logistic support, supplies, and services: an Acquisition-only Authority, and a Cross-Servicing Authority, which includes an acquisition authority and a transfer authority.

Acquisition-Only Authority. 10 U.S.C. Section 2341, "Authority to acquire logistic support, supplies, and services for elements of the armed forces deployed outside the United States," authorizes elements of the U.S. Armed Forces, when deployed outside the United States, to acquire logistic support, supplies, and services from eligible foreign entities on a reimbursable basis. The authority is not reciprocal and does not require the existence of a cross-servicing agreement or implementing arrangement. This is a very limited authority that has been mainly supplanted by the use of broader authorities in ACSAs. Acquisition-only authority may be used with the governments of NATO members, NATO and its subsidiary bodies, the United Nations

Organization, any regional organization of which the United States is a member, and any other countries which meet one or more of the following criteria:

- Has a defense alliance with the United States;
- Permits the stationing of members of the U.S. armed forces in such country or the home porting of naval vessels of the United States in such country;
- Has agreed to preposition materiel of the United States in such country; or
- Serves as the host country to military exercises which include elements of the U.S. armed forces or permits other military operations by the U.S. armed forces in such country.

Cross-Servicing Authority. 10 U.S.C. 2342, "Cross-servicing agreements," authorizes the Department of Defense, upon coordination with the Secretary of State, to conclude reciprocal agreements with foreign countries and regional and international organizations for the provision of logistics, support, supplies and services. A current listing of these agreements and countries and organizations eligible to negotiate them is maintained by the Director for Logistics, The Joint Staff (J-4). DoD Directive 2010.9 provides the official process for nominating countries for eligibility for such agreements as well as for concluding them.

11.2.3.2. Permitted and Prohibited Uses of Acquisition and Cross-Servicing Agreements (ACSAs)

ACSA is for the transfer of logistics, support, supplies, and services only. Per Section 4.5 of DoD Directive 2010.9, items that may not be acquired or transferred under ACSA authority include weapons systems; the initial quantities of replacement and spare parts for major end items of equipment covered by tables of organization and equipment, tables of allowances and distribution, or equivalent documents; and major end items of equipment. Specific items that may not be acquired or transferred under ACSA authority include guided missiles; naval mines and torpedoes; nuclear ammunition and included items such as warheads, warhead sections, projectiles, demolition munitions, and training ammunition; cartridge and propellant-actuated devices; chaff and chaff dispensers; guidance kits for bombs or other ammunition; and chemical ammunition (other than riot control agents). General purpose vehicles and other items of non-lethal military equipment not designated as Significant Military Equipment on the United States Munitions List promulgated pursuant to 22 U.S.C. 2778, may be leased or loaned for temporary use. Specific questions on the applicability of certain items should be referred to the Combatant Command's legal office for review and approval.

11.2.3.3. Repayment of Acquisition and Cross-Servicing Agreement (ACSA) Obligations

In addition to the use of cash and subject to the agreement of the parties, ACSA obligations may be reconciled by either Replacement-in-Kind or Equal Value Exchange. ACSA obligations not repaid by Replacement-in-Kind or Equal Value Exchange automatically convert to cash obligations after one year.

Replacement in Kind (RIK). RIK allows the party receiving supplies or services under the ACSA to reconcile their obligation via the provision or supplies and services of an identical or substantially identical nature to the ones received. As an example, a country may provide extra water to the United States during a training exercise with the proviso that the United States will provide the same amount of water during a future exercise.

Equal Value Exchange (EVE). EVE enables the party receiving supplies or services under the ACSA to reconcile their obligation via the provision of supplies or services that are considered to by both parties to be of an equal value to those received. As an example, a country may provide extra water to the United States during a training exercise in exchange for the United States providing extra ammunition.

11.2.3.4. Acquisition and Cross-Servicing Agreement (ACSA) Implementation

DoD Directive 2010.9 and CJCS Instruction 2120.01 provide management guidance on initiating ACSA orders, receiving support, reconciling bills, and maintaining records. As this is a Combatant Command-managed program, organizations interested in acquiring logistics, support, supplies and services should work through the applicable logistics branch to receive further guidance on this topic.

11.2.4. Summary of International Cooperation Guidance and Resources

International cooperation offers the opportunity to achieve cost savings from the earliest phases of Pre-Systems Acquisition throughout the life cycle, while enhancing interoperability with coalition partners. All DoD acquisition personnel, in consultation with the appropriate international programs organizations, should strive to identify and pursue international cooperative programs in accordance with DoD 5000 policy. Specific topics are found in the International Armaments Cooperation Handbook at the OSD/International Cooperation website.

11.3. Integrated Program Management

The program manager should obtain integrated cost and schedule performance data at an appropriate level of summarization to monitor program execution. The program manager should require contractors and government activities to use internal management control systems that accomplish the following:

- Relate time-phased budgets to specific tasks identified in the statement of work;
- Produce data that indicate work progress;
- Properly relate cost, schedule, and technical accomplishment; and
- Produce data that is valid, timely, and auditable.

Unless waived by the Milestone Decision Authority, the program manager should require that the management control systems used to plan and control contract performance comply with American National Standards Institute/Electronic Industries Alliance Standard 748, Earned Value Management Systems (ANSI/EIA-748, available for purchase) (see DoD Instruction 5000.02). The program manager should not impose a specific system or method of management control or require a contractor to change its system, provided it complies with ANSI/EIA-748.

11.3.1. Earned Value Management (EVM)

11.3.1. Earned Value Management (EVM)

EVM is a key integrating process in the management and oversight of acquisition programs, to include information technology projects. It is a management approach that has evolved from combining both government management requirements and industry best practices to ensure the total integration of cost, schedule, and work scope aspects of the program. Unless waived by the Milestone Decision Authority, EVM applies to contracts described below. The program manager's approach to satisfying the EVM requirement for applicable contracts should be documented in the program acquisition strategy. For more information on EVM, refer to the Office of the Secretary of Defense EVM web site, the Defense Contract Management Agency "Communicator" magazine, or the EVM Community of Practice web site on the Acquisition Community Connection knowledge sharing system.

11.3.1.1. Earned Value Management (EVM) Applicability

The requirement for EVM applies to cost or incentive contracts, subcontracts, intra-government work agreements, and other agreements that meet the dollar thresholds prescribed in DoD Instruction 5000.02. The application thresholds (total contract value including planned options in then-year dollars) are summarized below:

- $20 million but less than $50 million – EVM implementation compliant with the guidelines in ANSI/EIA-748 (available for purchase) is required. No formal Earned Value Management System (EVMS) validation is required.
- $50 million or greater – EVM implementation compliant with the guidelines in ANSI/EIA-748 is required. An EVMS that has been formally validated and accepted by the cognizant contracting officer is required.

The program manager will implement EVM on applicable contracts within acquisition, upgrade, modification, or materiel maintenance programs, including highly sensitive classified programs, major construction programs, and automated information systems. EVM should be implemented on applicable contracts wherein the following circumstances exist: (1) the prime contractor or one or more subcontractors is a non-U.S. source; (2) contract work is to be performed in government facilities, or (3) the contract is awarded to a specialized organization such as the Defense Advanced Research Projects Agency. In addition, EVM should be implemented on applicable contracts designated as major capital acquisitions in accordance with Office of Management and Budget Circular A-11, Part 7, and the Capital Programming Guide.

The application of EVM is not required on contracts, subcontracts, intra-government work agreements, and other agreements valued at less than $20 million (total contract value including planned options). The decision to implement EVM on these contracts is a risk-based decision at the discretion of the program manager. The program manager is required to conduct a cost-benefit analysis before deciding to implement EVM on these contracts. The purpose of the cost-benefit analysis is to explain the rationale for the decision to require cost/schedule visibility into the contract and to substantiate that the benefits to the government outweigh the associated costs. See the DoD Earned Value Management Implementation Guide (EVMIG) for additional guidance on applying EVM on contracts valued at less than $20 million. If the value of a contract is expected to grow to $20 million or more, the program manager should impose an EVM requirement on the contract.

The application of EVM is not required on contracts, subcontracts, intra-government work agreements, and other agreements less than 12 months in duration, including options. The decision to implement EVM on these contracts is a risk-based decision at the discretion of the program manager. If the duration of a contract is expected to grow to reach or exceed 12 months, the program manager should impose an EVM requirement on the contract.

The application of EVM on Firm-Fixed Price (FFP) contracts, subcontracts, intra-government work agreements, and other agreements is discouraged regardless of dollar value. If knowledge by both parties requires access to cost/schedule data, the first action is to re-examine the contract type (e.g., is a fixed price incentive contract more appropriate). However, in cases where

cost/schedule visibility is required, such as for development or integration efforts valued at or greater than $20 million, the program manager is required to obtain a waiver for individual contracts from the MDA. In these cases, the program manager is required to conduct a business case analysis that includes rationale for why a cost or fixed price incentive contract was not the proper contracting vehicle. When possible, the business case analysis should be included in the acquisition approach section of the program acquisition strategy. See the DoD EVMIG for additional guidance on applying EVM on FFP contracts.

If a contract type is mixed, the EVM policy should be applied separately to the different parts (contract types). See the DoD EVMIG for additional guidance on applying EVM on mixed type contracts.

As a general rule, EVM is required on cost or incentive contracts valued at or greater than $20 million; however, it may be necessary to consider the nature of the work associated with the contract when determining EVM applicability. In the EVM context, there are two basic classifications of the nature of work—discrete and level of effort (LOE). Discrete work is related to the completion of specific end products or services and can be directly planned, scheduled, and measured. LOE is effort of a general or supportive nature that does not produce definite end products (time and materials and services contracts may contain LOE work). The application of EVM on work that is LOE in nature may be impractical and inefficient. Therefore, if the work on a contract is exclusively LOE, it may be appropriate to request a waiver to the EVM policy from the program decision authority. When possible, waiver requests should be included in the program acquisition strategy. If EVM is waived for a contract due to the nature of the work, the program manager is required to implement an alternative method of management control to provide advanced warning of potential performance problems. See the DoD EVMIG for additional guidance on applying EVM on LOE work.

For Indefinite Delivery/Indefinite Quantity or task order types of contracts, the application of EVM based on dollar threshold is assessed at the computed total contract value and not by each separate order. To determine EVM applicability, anticipated cost or incentive orders should be summed to reach the computed total contract value. FFP orders are generally not included in that summation. See the DoD EVMIG for additional guidance on applying EVM on task order types of contracts.

11.3.1.2. Earned Value Management (EVM) Requirements

The program manager should use Defense Federal Acquisition Regulation Supplement (DFARS) clauses 252.234-7001 and 252.234-7002 to place the Earned Value Management System (EVMS) requirement in solicitations and contracts. The EVMS FAR clauses will not be applied to DoD contracts. The DFARS clauses, which have been deemed "substantially the same" as the FAR clauses, will be used instead of the FAR clauses (see DFARS 234.203). See the EVM Contract Requirements Checklist for additional information.

The contract should not specify requirements in special provisions and/or statements of work that are not consistent with the EVM policy and EVMS guidelines (required by imposition of DFARS 252.234-7002). Consult DCMA for guidance on compliance of the contractor's EVMS.

11.3.1.3. Integrated Baseline Reviews (IBRs)

An IBR is a joint assessment of the Performance Measurement Baseline (PMB) conducted by the government program manager and the contractor. The IBR is not a one-time event. It is a process, and the plan should be continually evaluated as changes to the baseline are made (modifications, restructuring, etc.). IBRs should be used as necessary throughout the life of a project to facilitate and maintain mutual understanding of:

- The scope of the PMB consistent with authorizing documents;
- Management control processes;
- Risks in the PMB associated with cost, schedules, and resources; and
- Corrective actions where necessary.

IBRs should be scheduled as early as practicable and the timing of the IBRs should take into consideration the contract period of performance. The process will be conducted not later than 180 calendar days (6 months) after: (1) contract award, (2) the exercise of significant contract options, and (3) the incorporation of major modifications. IBRs are also performed at the discretion of the program manager or within a reasonable time after the occurrence of major events in the life of a program. These events may be completion of the preliminary design review, completion of the critical design review, a significant shift in the content and/or time phasing of the PMB, or when a major milestone such as the start of the production option of a development contract is reached. Continuous assessment of the PMB will identify when a new IBR should be conducted.

In accordance with DoD Instruction 5000.02, program managers are required to conduct IBRs on all cost or incentive contracts that require the implementation of Earned Value Management (contracts valued at or greater than $20 million). However, conducting the IBR is not dependent on the contractor's Earned Value Management System being formally validated as complying with the guidelines in ANSI/EIA-748 (available for purchase). Subcontracts, intra-government work agreements, and other agreements also require IBRs as applicable. The scope of the IBRs should be tailored to the nature of the work effort.

The policy allows for the use of IBRs prior to contract award in situations where they may be appropriate and beneficial. If a program manager elects to conduct a pre-award IBR on a DoD contract, that requirement should be included in the statement of work.

See section 4.3.3.4.1 for more information on IBRs. See the Program Managers' Guide to the Integrated Baseline Review Process and the DoD Earned Value Management Implementation Guide for additional guidance on IBRs.

11.3.1.4. Contract Performance Management Reporting

The Contract Performance Report (CPR) and the Integrated Master Schedule (IMS) apply to all contracts that meet the Earned Value Management (EVM) applicability requirements in DoD Instruction 5000.02 . On contracts valued at or greater than $20 million but less than $50 million, it is recommended that CPR and IMS reporting be appropriately tailored. See the DoD Earned Value Management Implementation Guide for additional guidance on tailoring reporting.

A common, product-oriented Work Breakdown Structure (WBS) that follows the DoD Work Breakdown Structure Handbook (MIL-HDBK-881A) (current version at time of award) is required for the CPR, the IMS, and the Contractor Cost Data Report (CCDR). Except for high-cost or high-risk elements, the required level of reporting detail should not normally exceed level three of the contract WBS.

The CPR and the IMS for all Acquisition Category (ACAT) I programs are submitted directly to the EVM Central Repository (CR) by the reporting contractors. The EVM CR is the sole addressee on the Contract Data Requirements Lists for these reports. See the EVM CR Manual for additional guidance on the CR requirements.

The use of a standard electronic data exchange format is required for all reports unless disclosure of this information would compromise national security. All data will be in a readable digital format (e.g., pdf files are not acceptable). The Extensible Markup Language standard (Project Schedule Cost Performance Management message) is the preferred format. The American National Standards Institute X12 standard (839 transaction set) is also acceptable. On-line access to the data may be provided to augment formal submission.

11.3.1.4.1. Contract Performance Report (CPR)

The CPR provides contract cost and schedule performance data that is used to identify problems early in the contract and forecast future contract performance. The CPR should be the primary means of documenting the ongoing communication between the contractor and the program manager to report cost and schedule trends to date and to permit assessment of their effect on future performance.

The program manager obtains a CPR (DD Form 2734) on all cost or incentive contracts, subcontracts, intra-government work agreements, and other agreements valued at or greater than $20 million. The CPR is not typically required for cost or incentive contracts valued at less than $20 million, contracts less than 12 months in duration, or Firm-Fixed Price contracts for production efforts. The DoD Earned Value Management Implementation Guide (EVMIG) discusses some circumstances where the CPR may be appropriate for contracts in these categories.

Data Item Description DI-MGMT-81466 (current version at time of award)--(login, then URL: https://assist.daps.dla.mil/online/parms/mainframe.cfm?ident_number=206421) is used to obtain the CPR. The contracting officer and contractor should negotiate reporting provisions in the contract, including frequency and selection of formats, level of detail, submission dates, variance thresholds and analysis, and the contract Work Breakdown Structure to be used. The program manager should tailor the CPR to the minimum data necessary for effective management control on contracts valued at less than $50 million. See the DoD EVMIG for additional guidance on tailoring CPR reporting.

In exceptional cases, the contractor may determine that the performance measurement budget or existing contract schedule cannot be achieved and no longer represents a reasonable basis for management control. With government approval, the contractor may implement an Over Target Baseline (OTB) or Over Target Schedule (OTS). For cost-reimbursement contracts, the contract budget base excludes changes for cost growth increases, other than for authorized changes to the contract scope. The OTB/OTS creates additional budget to complete in-scope work, but it does not increase the negotiated contract cost.

11.3.1.4.2. Integrated Master Schedule (IMS)

The IMS is a time-based schedule containing the networked, detailed tasks necessary to ensure successful program/contract execution. The IMS is traceable to the integrated master plan, the contract Work Breakdown Structure, and the statement of work. The IMS is used to verify attainability of contract objectives, to evaluate progress toward meeting program objectives, and to integrate the program schedule activities with all related components.

The program manager obtains an IMS on all cost or incentive contracts, subcontracts, intra-government work agreements, and other agreements valued at or greater than $20 million. The IMS is applicable to development, major modification, and low rate initial production efforts; it is not typically applied to full rate production efforts. It is also not normally required for contracts valued at less than $20 million, contracts less than 12 months in duration, or Firm-Fixed Price contracts for production efforts. The DoD Earned Value Management Implementation Guide (EVMIG) discusses some circumstances where the IMS may be appropriate for contracts in these categories.

Data Item Description DI-MGMT-81650 (current version at time of award) is used to obtain the IMS. The contracting officer and contractor should negotiate reporting provisions in the contract, including level of detail, submission dates, and frequency of the schedule risk analysis. The program manager should tailor the IMS to the minimum data necessary for effective management control on contracts valued at less than $50 million. See the DoD EVMIG for additional guidance on tailoring IMS reporting.

11.3.1.5. Earned Value Management System (EVMS) Compliance, Validation, and Surveillance

The Defense Contract Management Agency (DCMA) is DoD's Executive Agent for EVMS. In its role as Executive Agent, DCMA has responsibility for EVMS compliance, validation, and surveillance.

11.3.1.5.1. Earned Value Management System (EVMS) Compliance and Validation

The requirements for EVMS compliance and validation are determined based on the Earned Value Management (EVM) application thresholds in section 11.3.1.1. The requirement for EVMS compliance applies to cost or incentive contracts, subcontracts, intra-government work agreements, and other agreements valued at or greater than $20 million. The basis for EVMS compliance is ANSI/EIA-748 (available for purchase). The contractor demonstrates EVMS compliance through the use of management processes and program reporting that are consistent with the guidelines in ANSI/EIA-748. The requirement for EVMS validation applies only to those contracts, subcontracts, intra-government work agreements, and other agreements valued at or greater than $50 million. Validation is achieved by conducting a formal review of the processes defined and used by the contractor to manage major acquisitions that assesses the capability of the contractor's proposed system to comply with the EVMS guidelines in ANSI/EIA-748. It determines that the contractor is using the system as one of its primary program management processes; that the contractor has properly implemented the system on the contract; and that the contractor is using the data from its system in reports to the government. See the DoD Earned Value Management Implementation Guide for additional guidance on EVMS compliance and validation.

11.3.1.5.2. Earned Value Management System (EVMS) Surveillance

Surveillance is required for all contract efforts that require the implementation of an EVMS compliant with the guidelines in ANSI/EIA-748 (available for purchase), regardless of whether a formal system validation is required. For the life of the contract, surveillance will be conducted on a recurring basis and should evaluate both the continuing capability of the contractor's EVMS and the validity of the internal and external performance information generated by the system. The results of surveillance efforts should be documented and identified deficiencies should be monitored and corrected. The responsibility and requirement for government surveillance of contracts should be based on the effectiveness of the contractor's implementation of internal management controls. See the Defense Contract Management Agency (DCMA)'s surveillance process for additional guidance on surveillance activity.

The Navy Supervisors of Shipbuilding have the authority to conduct EVMS surveillance activities, and the responsibility to coordinate with DCMA, for the contracts under their cognizance.

11.3.2. Other Contract Management Reporting

11.3.2. Other Contract Management Reporting

The reports described in this section apply to many defense contracts. They help to ensure effective program management.

11.3.2.1. Contract Funds Status Report (CFSR)

The CFSR supplies funding data about defense contracts to program managers for:

- Updating and forecasting contract funds requirements;
- Planning and decision making on funding changes in contracts;
- Developing funds requirements and budget estimates in support of approved programs;
- Determining funds in excess of contract needs available for deobligation;
- Obtaining rough estimates of termination costs; and
- Determining if sufficient funds are available by fiscal year to execute the contract.

The program manager will obtain a CFSR (DD Form 1586) on contracts over 6 months in duration. The CFSR has no specific application thresholds; however, the program manager should carefully evaluate application to contracts valued at less than $1.5 million (in then-year dollars).

DID DI-MGMT-81468 (current version at time of award) is used to obtain the CFSR. The contracting officer and contractor should negotiate reporting provisions in the contract, including level of detail and reporting frequency. The program manager should require only the minimum data necessary for effective management control. The CFSR should not be applied to Firm-Fixed Price contracts unless unusual circumstances dictate specific funding visibility.

The CFSR for all Acquisition Category I programs is submitted directly to the Earned Value Management Central Repository (CR) by the reporting contractors. The CR will be the sole addressee on the CDRL for this report. See the EVM CR Manual for additional guidance on the CR requirements.

The use of a standard electronic data exchange format is required for all reports unless disclosure of this information would compromise national security. All data will be in a readable digital format (e.g., pdf files are not acceptable). The Extensible Markup Language standard (Project Schedule Cost Performance Management message) is the preferred format. The American

National Standards Institute X12 standard (839 transaction set) is also acceptable. On-line access to the data may be provided to augment formal submission.

11.3.2.2. Cost and Software Data Reporting (CSDR)

The CSDR system is the primary means that DoD uses to collect actual cost and related business data on Acquisition Category I and IA and pre-MDAP and pre-MAIS defense contracts subsequent to Milestone A approval. DoD Instruction 5000.02 makes CCDR mandatory. Program managers use the CSDR system to report data on contractor development and production costs and resource usage incurred in performing DoD programs. Its two principal components are contractor cost data reporting (CCDR) and software resources data reporting (SRDR).

The Chair, Cost Analysis Improvement Group (CAIG) establishes procedural guidance and reporting formats for the CSDR system and monitors implementation throughout DoD. Detailed procedures and other implementing guidance are prescribed on the Defense Cost and Resource Center (DCARC) web site and have been incorporated into the CSDR Manual, DoD 5000.04-M-1.

Data Collection and Availability. CSDR data are collected and stored in a central repository, the Defense Automated Cost Information Management System (DACIMS), maintained by the DCARC. DACIMS has more than thirty five years of contractor cost data. DACIMS access is easy and quick for all authorized DoD users. Please refer to the DCARC web site and Chapter 5 of the CSDR Manual, DoD 5000.04-M-1, for specific registration instructions.

Purpose. The repository (DACIMS) may be used to obtain cost data to estimate total program acquisition costs (includes work by both contractors and the U.S. Government); total program contract costs (awarded and future) for a particular contractor (referred to as "contractor program estimates") and individual contract costs. Data may be used to:

- Prepare acquisition cost estimates for major system milestone reviews presented to Defense Acquisition Board (DAB) and Component acquisition executive at system milestone reviews
- Develop independent U.S. Government contract cost estimates in support of contract cost and price analyses
- Develop cost estimates to support analyses of alternatives, cost as an independent variable, and long-range planning efforts

Coverage. CSDR coverage generally extends from Milestone A approval to the completion of production.

Stakeholders. The key stakeholders in the CSDR process include: the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Office of Secretary of Defense (OSD), Cost Analysis Improvement Group (CAIG), Component Cost Centers, DoD Program

Managers, Cost Working-level Integrated Product Team (CWIPT), DCARC, reporting contractors, Defense Contract Audit Agency (DCAA), and the Defense Contract Management Agency (DCMA).

Reporting Formats and Instructions. The CSDR system includes two formats and instructions that apply to both CCDRs and SRDRs, four unique CCDRs, and three unique SRDRs. The two CSDRs are shown in this section while the unique reports are covered in the separate CCDR and SRDR sections below.

The DD Form 2794, "Cost and Software Data Reporting Plan" (commonly referred to as the "CSDR Plan") describes the proposed collection of data by individual report, by work breakdown structure (WBS) and reporting frequency. The plan must be approved by the Chair, CAIG prior to issuance of a contract solicitation. The Chair, CAIG, may waive the information requirements prescribed in Table 4 in Enclosure 4 of DoD Instruction 5000.02.

The format for the Contract Work Breakdown Structure is contained within the Data Item Description (DID) (DI-MGMT-81334, current edition). The CSDR Plan format and instructions and the link to the official DID can be found at the DCARC web site.

Training. The DCARC provides periodic CSDR training at various sites throughout CONUS for both government and contractor personnel. DCARC strongly encourages stakeholders to attend these training sessions and schedules classes to meet stakeholder requirements. The training schedule and various training materials can also be found at the DCARC web site.

11.3.2.2.1. Contractor Cost Data Reporting (CCDR) Specific Requirements

CCDR is the primary means within the Department of Defense to systematically collect actual data on the development and production costs incurred by contractors in performing DoD acquisition program contracts.

General Requirements. CCDRs are required on all major contracts and subcontracts, regardless of contract type, for Acquisition Category I and IA programs and pre-Major Defense Acquisition Program and pre-Major Automated Information System programs subsequent to Milestone A approval, valued at more than $50 million (Then year dollars). CCDRs are not required for contracts priced below $20 million (Then year dollars). The CCDR requirement on high-risk or high-technical-interest contracts priced between $20 and $50 million is left to the discretion of the DoD Program Manager (PM) based upon the advice of the Cost Working-level Integrated Product Team (CWIPT). These requirements must also be approved by the Chair, Cost Analysis Improvement Group (CAIG). CCDRs are not required under the following conditions provided the DoD PM requests and obtains approval for a reporting waiver from the Chair, CAIG: procurement of commercial systems or for non-commercial systems bought under competitively awarded, firm fixed-price contracts, as long as competitive conditions continue to exist.

Level of Reporting. Routine CCDR shall normally be at level 3 (level 4 for space contracts) of the Contract Work Breakdown Structure (WBS) and determined separately for each prime contractor and subcontractor that meets the reporting thresholds. Reporting at levels 4 and below shall be required on those prime contracts or subcontracts containing WBS elements that address high-risk, high-value, or high-technical-interest areas of a program. Such reporting applies only if the CWIPT proposes and the OSD CAIG Chair approves.

Report Timing. Initial reports are due within 60 days following the completion of the integrated baseline review when a pre-award or post-award conference is held. If a conference is not held, the initial report is due within 180 days of contract award. For subsequent reporting on development contracts, reporting contractors typically shall submit CCDRs after such major events as first flight or completion of prototype, before major milestones, and upon contract completion. In general, quarterly, semiannual, and annual reporting do not meet the above guidance. For production, reporting contractors normally shall submit CCDRs upon the delivery of each annual lot for all weapon systems. Due to the extended construction process for ships, CCDRs are also required for the total number of ships in each buy and for each individual ship within that buy at three intervals—initial report (total buy and individual ships), at the mid-point of first ship construction (individual ships only) or other relevant timeframe as the CWIPT determines, and after final delivery (total buy and individual ships).

Formats and Instructions. CCDRs consist of the DD Form 1921, "Cost Data Summary Report," DD Form 1921-1, "Functional Cost-Hour Report," DD Form 1921-2, "Progress Curve Report" and DD Form 1921-3, "Contractor Business Data Report." The related instructions are included in the DIDs for these forms as follows: DD Form 1921: DID, DI-FNCL-81565; DD Form 1921-1 DID, DI-FNCL-81566; DD Form 1921-2 DID, DI-FNCL-81567; and DD Form 1921-3 DID, DI-FNCL-81765. The forms including the Microsoft Excel templates and the link to the official DIDs are shown on the DCARC web site.

11.3.2.2.2. Software Resources Data Report (SRDR) Specific Requirements

The SRDR system collects software metrics data to supplement actual CCDR cost data to provide a better understanding and improved estimating of software intensive programs.

General Requirements. SRDRs are required on all major contracts and subcontracts, regardless of contract type, for contractors developing/producing software elements within Acquisition Category I and IA programs and pre-Major Defense Acquisition Program and pre-Major Automated Information System programs subsequent to Milestone A approval for any software development element with a projected software effort greater than $20M (Then year dollars). The SRDR requirement on high-risk or high-technical-interest contracts priced below $20 million is left to the discretion of the DoD Program Manager (PM) based upon the advice of the Cost Working-level Integrated Product Team (CWIPT). These requirements must also be approved by the Chair, Cost Analysis Improvement Group (CAIG).

Level of Reporting. The program office, in coordination with the CWIPT, may choose to combine a set of smaller releases within a contract into a single release for reporting purposes. Separate software element developments within a single contract may be reported on separately or may be aggregated at the discretion of the DoD PM based upon the advice of the CWIPT.

Report Timing. Within 60 days of contract award, the software developer shall be required to submit an SRDR Initial Developer Report for the entire software product, customized as agreed to by the DoD PM in coordination with the CWIPT. The software developer also shall be required to submit an SRDR Initial Developer Report for each deliverable software release or element within 60 days of the beginning of its development. In addition the software developer shall be required to submit an "as built" SRDR Final Developer Report, customized as agreed to by the CWIPT, within 60 days after delivery of each software release or element to the U.S. Government.

Formats and Instructions. SRDRs consist of the sample SRDR formats which are contained within the report instructions as follows: SRDR Sample Format 1, "Software Resources Data Reporting: Initial Government Report," SRDR Sample Format 2, "Software Resources Data Report: Initial Developer Report and Data Dictionary," and SRDR Sample Format 3, "Software Resources Data Report, Final Developer Report and Data Dictionary". The instructions for the Initial Government Report can be found on the DCARC web site. The instructions for the other two previously mentioned reports are contained in DIDs DI-MGMT-81739 and DI-MGMT-81740, respectively. The link to the official DIDs and the Microsoft Excel templates can also be found on the DCARC web site.

11.3.3. Quality Management

According to American National Standards Institute (ANSI), International Organization for Standardization (ISO), and American Society for Quality (ASQ), international standard ANSI/ISO/ASQ Q9000-2005 (ISO 9000), Quality Management Systems—Fundamentals and Vocabulary:

- Quality is the degree to which a set of inherent characteristics fulfils requirements. It may apply to a product or process. Inherent characteristics may be physical, sensory, behavioral, temporal, ergonomic, functional, etc.
- Quality management represents the organized activities to direct and control an organization with regard to quality.
- Quality assurance is the part of quality management focused on providing confidence that quality requirements will be fulfilled.

Effective quality management activities are important for reducing process-related risks to programs. Such risks include:

- Ill-defined or omitted requirements;
- A breakdown in requirements flow down;

- Uneconomically producible designs as a result of inappropriate application of technical processes;
- Inadequate procedures to implement contract requirements;
- Suppliers with inadequate capabilities;
- Decreasing leverage with sub tiers as a result of ineffective supplier management;
- Dissatisfied customers as a result of ineffective customer engagement; and/or
- Undetected product defects resulting from unidentified verification technologies or failure to implement existing ones.

If not managed and mitigated, these risks may start a chain of events leading to undesirable outcomes such as:

- Product defects discovered in production or testing that may require expensive and time-consuming rework
- Products that may not meet customer needs
- Product deficiencies discovered in the field that may lead to degraded mission effectiveness, early wear out or mishaps
- Cost overruns or delays for current contracts and
- Cost escalation for future contracts
- Parts shortages at the wholesale and retail levels

The later these risks are identified, the greater the cost of corrective action and the greater the delays in schedule. Early identification, management, and mitigation of important process-based risks to a program lead to less expensive and less disruptive corrective actions that break the chain of undesirable outcomes.

While the DoD program manager should encourage and support the contractor's efforts to assure quality, ultimately, the prime contractor is responsible. Therefore, from a DoD perspective, a key program success factor is selecting contractors that can demonstrate effective quality management. This subject is discussed in section 11.3.3.1.

The contract should provide incentive to the contractor to deliver products or services that provide value beyond the basic requirement. Without additional incentives, the systems engineering process will normally lead to decisions that satisfy requirements at the lowest cost. It may however be possible to incentivize the contractor to (1) exceed a basic requirement such as mean time between failures or (2) generate a higher level for an important derived requirement (e.g., one that affects operational flexibility, maintainability, supportability, etc.). Section 11.3.3.2 discusses this topic.

Applying best practices as described in Sections 11.3.3.1 and 11.3.3.2 may not be sufficient to manage and mitigate the process-based risks list above. Section 11.3.3.3 discusses how encouraging a quality focus can also contribute.

Government Contract Quality Assurance (GCQA) determines if contractual requirements have been met prior to acceptance of supplies and services. GCQA is conducted by the program manager and Defense Contract Management Agency (DCMA) as identified in contract administration delegations to DCMA by the Contracting Officer. Section 11.3.3.3 discusses some best practices for setting quality assessment and oversight requirements for the GCQA function, tailored to the expected risks.

11.3.3.1. Differentiating Among Offerors on the Basis of Quality

11.3.3.1. Differentiating Among Offerors on the Basis of Quality

A contractor's quality management system is used to direct and control the organization with regard to quality. Quality management is an enterprise level process, driven by senior leadership involvement, to support the delivery of high quality products and services by ensuring that all aspects of quality are considered and acted upon by every element of the organization. The fundamental goal is to provide objective insight to assure that: customer requirements are thoroughly analyzed and understood; processes are defined and capable; and the resulting product meets the customer's needs. It interacts with systems engineering technical processes and technical management processes by focusing on both the quality of the system and the quality of the processes being used to create the system. Quality management provides objective insight into processes and work products for all stakeholders including program team members, management, suppliers, customers, and users involved with the development, manufacture, operation, and support of a system.

The quality management process begins early in the life cycle and continues throughout. The principal elements of the quality management process include:

- Objectively evaluating performed processes, work products, product/process design and services against the applicable process descriptions, standards, procedures, policies, and documented expectations;
- Understanding the full scope of customer requirements, assessing risks associated with meeting those requirements, and verifying that they are satisfied;
- Identifying and documenting noncompliance issues, especially those affecting cost, schedule, productivity, and performance;
- Using tools and techniques in a disciplined manner to determine root causes of noncompliance issues;

- Addressing noncompliance issues by initiating and tracking corrective and preventative actions to assure the root cause(s) of the defect/deficiency has been identified and removed; and
- Providing feedback to program managers, their staff, and corporate managers to identify lessons learned, improve process robustness for future projects, and evaluate trends.

While the quality management focus is on the key aspects of the product realization process (e.g., requirements, design, make/buy decisions, supplier management, production), it also encompasses supporting processes such as contracting and training. Both value-added activities and continuous process improvement should be stressed and encouraged.

Further information about quality management may be found in ISO 10005 Quality Management - Guidelines for Quality Plans (available for purchase), AQAP-2000 NATO Policy on an Integrated Systems Approach to Quality through the Life Cycle, AQAP-2009 NATO Guidance on the Use of the AQAP 2000 Series, and at Process and Product Quality Assurance in the CMMI for Development (CMMI-DEV) v1.2 or the CMMI for Acquisition (CMMI-ACQ) v1.2.

Program managers should allow contractors to define and use their preferred quality management system as long as it meets the needs of the program. International quality standard ISO 9001-2008, Quality Management Systems - Requirements, AQAP-2110, NATO Quality Assurance Requirements for Design, Development and Production, and AS 9100C:2009, Aviation, Space and Defense Quality Control Management System Standard, define process-based quality management systems and are acceptable for use on contracts per FAR 46.202-4, Higher-Level Contract Quality Requirements. AQAP-2110 and AS 9100 contain additional requirements beyond ISO 9001. AS 9100 is applicable to most complex DoD systems. The AQAP 2000 series should be considered for complex DOD systems, when the supply chain or the end products have NATO or international implications. Program managers should consider the use of additional requirements (such as those contained in the Missile Defense Agency Assurance Provisions) beyond ISO 9001 as appropriate.

Other sector specific quality management systems acceptable under FAR 46.202-4 include:

- TL 9000, Quality System Requirements for the telecommunications industry
- ISO/IEC 90003:2008, Software engineering -- Guidelines for the application of ISO 9001:2000 to computer software (available for purchase)
- QS-9000 or ISO/TS 16949:2009 (available for purchase), ISO 9000 harmonized standards for automotive suppliers of production materials and service parts in North America

To improve a contractor's quality management system, standards bodies encourage registration based upon an impartial third party evaluation. The Department of Defense does not require registration of a contractor's quality management system because registration does not guarantee product or service quality. Reasons why the Department of Defense does not require registration include the following:

- Registrars (auditors) do not look at the product;
- There have been instances where a registered contractor delivered a deficient product;
- Many companies pursue registration of their quality management system as a goal in itself or as a marketing tool; and
- Some registrars are less demanding.

Compliance to a standard such as ISO 9001 (available for purchase), AQAP-2000, AQAP-2009, or AS 9100, does not, in itself, guarantee product or service quality. These standards are management system standards that identify requirements for processes within an organization, describe expected tasks and outcomes, and explain how the processes and tasks integrate to produce required inputs and outputs. Standards are meant to enable the organization to develop a set of processes that, if done by qualified persons using appropriate tools and methods with appropriate leadership involvement, will enable a capability for delivering high quality products or services.

Product or service quality is achieved through the implementation of a strategic plan to integrate all business and technical functions that result in the consistent application of proven, capable processes within an organization. Managers must ensure that all management systems are working toward the same goals and are not creating conflicting or dysfunctional behavior. Implementing a standard is of little use if the financial system rewards individuals for delivering non-conforming products/services. Because everything a contractor does should be related to the quality of its products or services, a contractor's quality management system should be the basis for integrating all other management systems within an enterprise. Therefore, include quality management as a selection factor and look for the following elements of a quality management system in proposals:

- Effective policies and procedures that encourage the use of the system;
- Organizations with defined authorities and responsibilities;
- Objectives to drive people, processes, and the system;
- Method to analyze and resolve quality problems;
- Metrics that reflect desired outcomes;
- Interacting processes to transform inputs into outputs; and
- Records as evidence of what happened.

Furthermore, to the extent that they are available, metrics that show the effectiveness of the contractor's quality management system and processes over time should also be used to differentiate among offerors.

The following subsections describe several broad areas that have had a significant impact on quality. Topics include Customer Satisfaction, Supply Chain Quality Management, Top Management Involvement, and Continual Improvement of Performance. They provide additional guidance on items the program office and the contracting office should ask for in Requests for Proposals and evaluators should look for in proposals to make a better assessment of a contractor's quality. These items may be used to differentiate among offerors. Depending on the

specific situation, there may also be other areas (e.g., competent personnel for special processes) where information should be sought.

11.3.3.1.1 Customer Satisfaction

Customer satisfaction, when quantified, is a valuable enterprise-level outcome metric. The Department of Defense has recognized the importance of customer-satisfaction performance measures. Since the passage of the Federal Acquisition Streamlining Act of 1994, all Federal Departments and Agencies have initiated procedures to record contractor performance on in-process contracts and to use past contractor performance information in source selection.

Too often in the past, the Department of Defense relied heavily upon detailed technical and management proposals and contractor experience to compare the relative strengths and weaknesses of offers. This practice often allowed offerors that could write outstanding proposals, but had less than stellar performance, to "win" contracts even when other competing offerors had significantly better performance records and, therefore, represented a higher probability of meeting the requirements of the contract. Emphasizing past performance in source selection, can help ensure that the winning teams (prime contractors and major subcontractors) are likely to meet performance expectations. When evaluating past performance data, consideration should be given to the relevancy, complexity and ultimate mission success of the contract.

Beyond the Department's past performance information, a Request for Proposals may ask for further evidence of customer satisfaction such as data tabulated from customer surveys or from complaints and equally important, how changes were made because of the results.

Supplier assessment programs may also be helpful in understanding how well a company is able to satisfy its customers. Suppliers have demonstrated some degree of customer satisfaction when they are accredited by a group of companies, in a particular sector, that joined together to agree on criteria and a process for assessing, exchanging and publishing supplier data to facilitate business relationships. For example, Nadcap is a worldwide cooperative program of major companies designed to manage a cost effective consensus approach to special processes and products and provide continual improvement within the aerospace industry; the Coordinating Agency for Supplier Evaluations (C.A.S.E.) exchanges and publishes non-prejudicial supplier data to help make informed supplier selections. Reports from consumer organizations or the media may also be useful.

11.3.3.1.2 Supply Chain Quality Management

Because quality deficiencies for non commercial-off-the-shelf (COTS) products often occur in the lower tiers, prime contractors should have insight at least two levels down their supply chain. Prime contractors, in addition to having approved vendor (i.e., subcontractor) lists, should ask their subcontractors' about planned suppliers. These subcontractors should also have insight two

levels down their supply chain and flow the same requirement down to their suppliers, etc. For COTS products, all contractors should use approved sources.

It is important for DoD program managers to inform their prime contractors of their interest in quality throughout the supply chain. Therefore, through requests for proposals and corresponding proposal evaluation factors, the program office and the contracting office should request and evaluate evidence of effective supply chain management. The evidence should reflect the following characteristics:

- Relationships with suppliers that promote and facilitate communication to improve the effectiveness and efficiency of processes that add value;
- The use of supplier development programs focused on continuous improvement;
- Strategic partnerships with suppliers, over the product life cycle, that are based on a clear understanding of the partners' and customers' needs and expectations in order to improve the joint value proposition of all stakeholders;
- Processes that effectively and efficiently monitor, evaluate, verify, and improve the suppliers' ability to provide the required products with a focus on defect prevention rather than defect detection;
- Right of access for both the prime contractor and the Government to supplier facilities and documentation where applicable; and
- Requirements for the supplier to flow down analogous quality management system provisions to its subcontractors.

Because quality deficiencies often occur in the lower tiers, prime contractors, in addition to having approved vendor (i.e., subcontractor) lists, should ask their subcontractors' about planned suppliers. These subcontractors should flow the same requirement down to their suppliers, etc. For critical and complex commercial-off-the-shelf (COTS) products, the prime and its subcontractors should use their own internal processes and controls to ensure that the COTS product meets its critical attributes.

11.3.3.1.3 Top Management Involvement

Quality will permeate all levels of a company only if top management provides the leadership necessary to drive and reinforce that behavior. Requests for Proposals should also ask for evidence of top management support for quality. The following list identifies important factors in evaluating the effectiveness of top management support:

- Establishing a corporate strategic vision, objectives, policies and procedures that reflect a commitment to quality both in-house and in suppliers' facilities;
- Communicating, at every opportunity, organizational direction and values regarding quality;
- Providing structures and resources to support full implementation of a quality management system;

- Soliciting quantitative and qualitative feedback on the effectiveness and efficiency of quality management and taking actions based on that feedback, even when change may be difficult;
- Establishing a quality policy, at the highest level in the company, that commits to continuously improving processes and exceeding customer expectations;
- Reviewing the quality management system periodically with particular attention paid to achieving goals and objectives throughout the organization, customer satisfaction, and the exchange of ideas for continuous improvement;
- Setting ambitious quality objectives and promulgating them through quality policy;
- Demonstrating importance put on quality functions by providing for independent reporting channels; and
- Establishing management accountability with emphasis on quality results and customer satisfaction.

11.3.3.1.4 Continual Improvement of Performance

An offeror with effective quality management will seek continual improvement of its processes, product designs, and thereby products by improving its overall performance, efficiency, and effectiveness. Such behavior increases the likelihood of increasing customer satisfaction and enhancing an organization's competitive posture.

More specifically, all processes have defined inputs and outputs as well as the required activities, actions and resources. Therefore, process improvement encompasses both:

1. Improving conformance to the defined process and
2. Improving the defined process itself to add value and eliminate waste.

Such process improvement invariably leads to (work and end) product improvement and consequently increased customer satisfaction.

When asking for evidence of a strong commitment to continual improvement in a request for proposal, the following list provides considerations for evaluating a response.

- How conditions are created to promote innovation,
- How open two-way communications are encouraged,
- How corrective actions are treated as an improvement tool,
- How change is approached on a systematic, consistent basis, to include follow-through implementation, verification and documentation,
- How people are provided with the authority, technical support and necessary resources for change,
- How continuous improvement process tools are deployed company-wide,
- How self assessments, benchmarking, competitor analysis, and other metrics are used to evaluate process performance and drive improvement, and

- How capability and maturity models or reviews support an effective continual improvement process and provide both insights to the improvement process itself and objective evidence of success.

11.3.3.2 Incentivizing Higher Quality in Contracts

Contract incentives can be structured to ensure quality by contributing to the contractor's value proposition. Factors that are typically important aspects of a contractor's value proposition include:

- Customer satisfaction;
- Planning stability;
- Good financial performance; and
- Improved cash flow.

Listed below are examples of contract incentives that can be made available to the prime contractor and the prime contractor can in turn make available to subcontractors under the appropriate conditions:

- Increased fee;
- Extended contract length;
- Follow-on contracts awarded;
- Accelerated progress payments;
- Shared savings; and
- Opportunities for return on investments (some of which may increase the contractor's competitiveness on other contracts).

The following are some potential ways to use these contract incentives to improve quality, and at the same time, improve other product characteristics that are of value to DoD. Their applicability depends on the specific situation.

- Warranties. The program manager could treat the warranty as a fixed price option per item. If there are no failures, the contractor keeps the money that DoD paid for the warranty. To reduce the price of the warranty, the program manager could consider a situation where DoD pays to repair the first failure and the contractor warranties the next "n" failures. Typically the warranty should exclude combat damage, abuse, misuse, and other factors out of the contractors' control.
- Award Fee for Product Support Contracts. The program manager could make the fee a function of operational availability.
- Award Fee for Product Development Contracts. The program manager could make the fee a function of successful operational test and evaluation.
- Progress Payments. The program manager could make payments contingent on successful corrective actions taken to alleviate quality deficiencies. The program manager could also establish an agreement with the contractor to repay the fee with interest if

future measurements do not meet the conditions necessary for the entire amount of the fee to be awarded.
- Share of Savings. The contract could encourage the contractor to invest in facilities, non recurring engineering, technology insertion, etc. that will result in improved performance and reduced costs. The program manager could then use the value engineering clause to repay the investment and give the contractor a share in the savings generated.

In building such relationships, the program manager should avoid actions that encourage risky behavior by the contractor. For example, by insisting on reducing cost, accelerating the schedule, improving performance beyond demonstrated technology limits, etc. the contractor may be forced to forgo quality-related processes. This may not only defeat the purpose of contractual incentives but also negate the other quality activities discussed in this section.

11.3.3.3 Encouraging a Quality Focus

Applying best practices as described in sections 11.3.3.1 and 11.3.3.2 may not be sufficient to manage and mitigate process-based risks that may start a chain of events leading to undesirable outcomes. DoD should also stress the importance of effective quality management to industry. By encouraging a quality focus, DoD can help avoid mismatches among value, beliefs, and behaviors. DoD should therefore encourage and participate with industry to apply effective practices in the following areas.

At Program Startup

- The process for establishing the product or project quality budget,
- Where quality responsibility is placed in the program,
- How quality skills have been assigned to the project,
- The process for analyzing quality requirements and mitigating associated risks, and
- The quality strategy's consistency with industry best practices.

Throughout the Life Cycle

- How management uses quality data,
- The contractor's approach for continuous process improvement,
- The contractor's approach for preventive and corrective action, and
- The contractor's approach for achieving customer satisfaction.

Evaluation considerations for each of the above areas are shown below:

- The process for establishing the product or project quality budget,
- Project quality administration, product verification, quality engineering (hardware and software), quality planning, and supplier quality,
- Specific quality deliverables,
- Capital, equipment, and software verification needs,

- How the estimates are modified when there are changes to the strategy and/or scope of the program, and
- Measurement technology needs.

Where quality responsibility is placed in the program:

- Role in the general risk identification, classification, and mitigation process,
- Involvement in the design change control and release process,
- Role in processing waivers, deviations and engineering change proposals,
- Representation on Integrated Process Teams and boards (e.g., change control board, risk) for all product and process development activities,
- Involvement in test plans, material reviews, design reviews, build/buy/support to packages,
- Participation in the integration of inspection points into processing and test documentation, and
- Role in the supplier management, development, incentivization, and control process.

How quality skills have been assigned to the project

- The process to identify the need for quality management, quality engineering (hardware and software), quality planning, supplier quality, and product verification skills across the life cycle,
- The process to identify quality skills and any associated certifications and qualifications, and
- The process for addressing quality staffing ratios and skill shortfalls

The process for analyzing quality requirements and mitigating associated risks:

- The process for identifying and achieving quality tasks in support of contract deliverables,
- How a post award contract analysis for Quality's tasks was performed / has been updated,
- An evaluation of how the Quality plan matches the program requirements and their integration across program sites, IPTs, partners and suppliers, and
- How quality activities factored into the Integrated Master Plan and Integrated Master Schedule.

The quality strategy's consistency with industry best practices:

- The use of lessons learned,
- How similar programs' quality past performance have been reviewed,
- How the quality plan addresses program unique processes,
- How plans include verification approaches, nonconformance handling, operator verification manufacturing self-examination, nondestructive inspection, manufacturing systems, measurement approach, special measuring and test equipment,

- Adequacy of the quality plan to address all other program plans (manufacturing, systems engineering, subcontract management, delivery, etc),
- Periodic review and update, and
- Early involvement in the program

How management uses quality data

- Audit needs and addressing audit findings,
- The process for analyzing and performing trend analysis of internal/external audit findings, and
- How quality is defined, measured, analyzed, controlled, and used to drive management decisions and actions on the program
    - The process for developing and identifying requirements for quality metrics and measurement systems
    - The system for monitoring supplier performance, including their product development activities
    - The process for review and update

The contractor's approach for continuous process improvement:

- Baldridge business model,
- CMMI,
- Lean,
- Six sigma,
- ISO recertification, and
- Actions taken to address feedback from assessments performed.

The contractor's approach for preventive and corrective action:

- The process for addressing test and inspection findings and discrepancies,
- The process for addressing supplier non-conformances,
- Establishment and maintenance of a closed loop corrective action system that includes the reporting, root cause analysis, and implementation of actions necessary to correct and preclude recurrence of problems, failures, quality issues, defects/non-conformances, and
- The process for using lessons learned to drive continuous improvement.

The contractor's approach for achieving customer satisfaction:

- The process to collect, monitor, and analyze information for measuring customer satisfaction,
- The process to rapidly mitigate customer concerns,
- The process to communicate with customers at all levels, and
- The process / organizational structure for reacting to customer inquiries and needs.

The program managers and responsible technical authority will utilize DoD preferred method of acceptance as reflected in MIL-STD-1916, *DoD Preferred Method of Acceptance*, (login, then URL: https://assist.daps.dla.mil/online/parms/mainframe.cfm?ident_number=120287), to allow contractors the maximum degree of flexibility to meet product or service requirements. The preferred method is acceptance by contractor-proposed provisions based on prevention-based strategies and process controls. The theme is partnering between Government and contractor to develop an optimal acceptance method for products and services that is consistent with the contract requirements for submission of all conforming products or services.

Prior to achieving effective prevention-based strategies and process controls, MIL-STD-1916 provides standardized acceptance sampling systems which are consistent with the contract requirements for submission of all conforming products or services. These sampling systems allow program managers to influence continuous improvement through corrective action while still allowing maximum degree of flexibility to contractors.

International quality standard ISO 21247, *Combined Accept-Zero Sampling Systems and Process Control Procedures for Product Acceptance*, (available for purchase) is an acceptable alternative to MIL-STD-1916.

11.3.3.4 Government Contract Quality Assurance (GCQA)

11.3.3.4 Government Contract Quality Assurance (GCQA)

GCQA is a joint responsibility between the program office and Defense Contract Management Agency (DCMA). Interdisciplinary skills (such as quality assurance, industrial specialist, engineering, and software) are needed.

The program manager should establish open and effective communication with DCMA. DCMA uses Contract Data Package Recommendation/Deficiency Reports (DD Form 1716) for the following:

- To improve contract data packages;
- When essential information is required as a basis for inspection/acceptance or shipment is incorrect, incomplete, unclear or unavailable; or
- When there is a conflict, ambiguity, noncompliance or other problem area between the contractor and Government concerning contractual requirements.

The DD Form 1716 is an important avenue of communication for DCMA to resolve contractual issues with the Procuring Activity and to understand and meet expectations and needs of their customers.

For item-managed contracts, Defense Logistics Agency ICPs issue Quality Assurance Letters of Instruction to DCMA to provide additional contractor past performance history and to request tailored or specialized surveillances during contract performance.

11.3.3.4.1 Formulating the Government Contract Quality Assurance Approach

For defense acquisition programs, the program manager should conduct a customer outcome strategy meeting (i.e., a post award conference) soon after the Systems Development and Demonstration contract award. At this meeting, the participants should:

- Identify desired customer/user expectations and outcomes,
- Determine the program risks that may negatively impact those outcomes,
- Analyze those risks to assess the potential consequences, and
- Define performance measures associated with the desired outcomes.

The program manager should ensure that some of these performance measures relate to key processes in the acquisition framework. For example, the performance measures should be linked to the entrance and exit criteria of the systems engineering technical reviews and the Milestone programmatic reviews during both the Systems Development and Demonstration Phase and the Production and Deployment Phase of the acquisition management framework.

The program manager should form a GCQA team and allow it the flexibility to formulate a risk-based quality assurance surveillance strategy designed to ensure that customer outcomes are achieved. The surveillance strategy should focus on the effectiveness of the contractor's product realization process which includes:

- Planning of Product Realization;
- Customer-Related Processes;
- Design and Development;
- Purchasing and Supplier Management;
- Production and Service Provision;
- Control of Monitoring and Measuring Devices; and
- Inspection, Test, Verification and Validation.

The surveillance strategy should also cover the contractor's continual improvement process. To be effective, this process should be data driven and the data should (1) be used to address both actual and predicted problems, and (2) should be revised to remain connected to process changes. In addition, include both periodic audits of the contractor's quality management system as well as

product examinations in the surveillance strategy. Both independence and the use of criteria in conducting audits and surveillance are critical to providing objective, meaningful insight.

As performance data are collected, the GCQA team should adapt the surveillance strategy based on risks identified and the need for special surveillance of critical safety items, critical characteristics or processes, mission critical items, key characteristics, etc. When planned results are not achieved, the program manager should ensure that preventive and corrective actions are developed and implemented. The GCQA team should extend the surveillance to verify that such actions accomplished their objectives.

11.3.3.4.2. Government Contract Quality Assurance (GCQA) Inspections

For item-managed contracts, detailed guidance on when to require GCQA at source or destination is contained in the Federal Acquisition Regulation (FAR), Part 46.

Per FAR Parts 46.402 and 46.404, the program manager shall use destination inspection for contracts or purchase orders under $250,000 for the reprocurement of items with no significant technical requirements, no critical characteristics, no special features, and no specific acquisition concerns, and where there is confidence in the contractor. Such inspections are limited to kind, count and condition. This may involve preservation, packaging, and marking (if applicable). Put FAR 52.246-1 on the contract. Use FAR 52.246-2 without FAR 52.246-11 only in those rare circumstances where there is reason to believe that there may be a problem.

Typically, source inspection is appropriate for complex / critical items where:

- The verification of technical characteristics requires in-process controls;
- Product quality cannot be adequately determined through basic end item product examination; or
- The contractor is experiencing or exhibiting difficulty controlling product characteristics.

The program manager should put both FAR 52.246-2 and FAR 52.246-11 (or FAR 52.246-8 for research and development programs) on the contract. FAR 52.246-2 allows Government access to the facility and requires the contractor to develop and maintain an inspection system. FAR 52.246-11 requires the contractor to implement a higher level quality management system. The responsible technical authority should prepare a Quality Assurance Letter of Instruction through the contracting officer to ensure that appropriate product specifications, drawings, and inspection and test instructions, including critical characteristics, are available and/or identified for use by the Defense Contract Management Agency. GCQA at the source encompasses one or more of the following based on defined risk:

- *Product Examinations:* Examinations of product characteristics to ensure they meet contract requirements. Depending on the identified risks, the Government CQA surveillance strategy might include various product examination techniques, such as

inspecting, testing, witnessing, verifying by use of objective evidence, and analyzing Government or contractor performance data.

- *Process Reviews:* Reviews to determine the suitability, adequacy, and effectiveness of the process to achieve product outputs that meet contract requirements.
- *System Assessments/Audits:* Systematic, independent assessments and audits of the various elements of the contractual quality management system impacting process or product quality.
- *Management and program reviews and meetings:* Maintains open channels of communication.

11.3.3.4.3. Government Contract Quality Assurance (GCQA) for Critical Safety Items (CSIs)

Special attention must be paid to CSIs regardless of whether they are item-managed or program-managed. Defense Federal Acquisition Regulation Supplement (DFARS) 246.103 states that the activity responsible for technical requirements may prepare instructions covering the type and extent of Government inspections for acquisitions that have critical applications (e.g., safety) or have unusual requirements. Section 4.4.21 discusses CSIs as a systems engineering design consideration. It provides a definition and links to some additional reference material.

The contracting officer should clearly mark the front page of the solicitation/contract with the words "Critical Safety Item." This raises the alertness level and makes everyone aware that CSIs are involved in the contract. When CSIs are determined after contract award, the responsible technical authority should use the words "Critical Safety Items" in the subject line of a Quality Assurance Letter of Instruction (QALI). All critical and major characteristics, the extent of inspection required, and the associated acceptance criteria should be described either in the contract or in the QALI. In addition, the technical authority should provide criteria for special inspections, process verification, or similar requirements. Acceptance criteria should also include additional instructions for situations where a CSI is purchased from a distributor, a CSI is purchased on a commercial contract, or CSI critical characteristics cannot be fully examined at a prime contractor's facility. To assure the communications loop is closed with Defense Contract Management Agency (DCMA), the QALI should request acknowledgement and DCMA acceptance of duties included within. The form should be returned to the responsible technical authority that transmitted the QALI.

Public Law 108-136, "National Defense Authorization Act for FY04," Section 802, Quality Control in the Procurement of Aviation Critical Safety Items and Related Services, "… requires that the head of the design control activity for aviation critical safety items establish processes to identify and manage the procurement, modification, repair, and overhaul of aviation critical safety items." DoD procedures for managing aviation CSIs are contained in Joint Service instruction, "Management of Aviation Critical Safety Items," and the Joint Aeronautical Logistics Commanders' Aviation Critical Safety Items (CSIs) Handbook. Additionally, per DFARS 246.407, the head of the design control activity is the approval authority for acceptance

of any nonconforming aviation critical safety items or nonconforming modification, repair, or overhaul of such items.

DCMA relies on the Procuring Activity's knowledge and involvement to determine whether an item is correctly categorized as a critical item. If DCMA questions the critical categorization of an item, the lack of a critical characterization of an item, or a CSI designation, DCMA will contact the Procuring Office to discuss the reasons behind the decision, gain a better understanding of the situation or customers needs, and request additional information. The Procuring Office should contact DCMA personnel whenever they have a concern, question, or possess additional information important to achieving customer outcomes.

11.4. Risk Management

The program manager and others in the acquisition process should take an active role in identifying and understanding program uncertainties, whether they have a negative or positive impact on the program baseline. An assessment of cost, schedule, or performance against a program baseline is not credible or realistic if uncertainties are not recognized and in some manner incorporated into estimates and assessments in a transparent manner.

The impact of uncertainty in particular areas of the program, on particular estimates and assessments, should be analyzed and understood.

To obtain additional information related to Risk Management such as: various risk management processes, assessment techniques, handling methods, and monitoring tools, go to the Risk Management Community of Practice at the Acquisition Community Connection; or go to the Risk Management Guide for DoD Acquisition. To obtain information on Environment, Safety, and Occupational Health (ESOH) risk management go to section 4.4.7 and 4.4.7.5; for ESOH risk reporting requirements go to section 4.4.7.6; and, for ESOH risk acceptance and user representative coordination requirements go to section 4.4.7.7.

11.5. Knowledge-Based Acquisition

Knowledge-based acquisition is a management approach which requires adequate knowledge at critical junctures (i.e., knowledge points) throughout the acquisition process to make informed decisions. DoD Directive 5000.01 calls for sufficient knowledge to reduce the risk associated with program initiation, system demonstration, and full-rate production. DoD Instruction 5000.02 provides a partial listing of the types of knowledge, based on demonstrated accomplishments, which enable accurate assessments of technology , design maturity , and production readiness.

Implicit in this approach is the need to conduct the activities that capture relevant, product development knowledge. And that might mean additional time and dollars. However, knowledge

provides the decision maker with higher degrees of certainty, and enables the program manager to deliver timely, affordable, quality products.

The following knowledge points and ensuing considerations coincide with decisions along the acquisition framework:

Program Initiation. Knowledge should indicate a match between the needed capability and available resources before a program starts. In this sense, resources is defined broadly, to include technology, time, and funding.

Considering the knowledge associated with technology, the knowledge should be based on demonstrated accomplishments. If a technology is not mature, the DoD Component must use an alternative technology or discuss modifying requirements with the users. By requiring proven technology before a program starts, we reduce uncertainty. Rather than addressing technology development and product development, the program manager and Milestone Decision Authority can focus on product development, because they know the technology is available. DoD Instruction 5000.02 enforces this concept with the following policy:

> *Technology developed in S&T or procured from industry or other sources shall have been demonstrated in a relevant environment or, preferably, in an operational environment to be considered mature enough to use for product development (see the "Technology Readiness Assessment (TRA) Deskbook" . . . . Technology readiness assessments, and where necessary, independent assessments, shall be conducted. If technology is not mature, the DoD Component shall use alternative technology that is mature and that can meet the user's needs or engage the user in a dialog on appropriately modifying the requirements.*

Post-Critical Design Review Assessment. Knowledge should indicate that the product can be built consistent with cost, schedule, and performance parameters. This means design stability and the expectation of developing one or more workable prototypes or engineering development models. DoD Instruction 5000.02 lists the specific factors that contribute to such knowledge.

Production Commitment. Based on the demonstrated performance and reliability of prototypes or engineering development models, knowledge prior to the production commitment should indicate the product is producible and meets performance criteria. DoD Instruction 5000.02 lists some of the specific factors that contribute to such knowledge.

Full-Rate Production Decision. Based on the results of testing initial production articles and refining manufacturing processes and support activities, knowledge prior to committing to full-rate production should indicate the product is operationally capable; lethal and survivable; reliable; supportable; and producible within cost, schedule, and quality targets.

11.6. Implementing a Performance-Based Business Environment (PBBE)

A PBBE relates the business considerations of the acquisition strategy to the Life-cycle considerations of Systems Engineering, Life-Cycle Logistics, and Human Systems Integration. The following considerations apply:

- As part of acquisition reform, the Military Departments and Defense Agencies reviewed all military specifications and standards, canceling unnecessary documents, replacing many with non-government standards, and rewriting others to state requirements in performance terms. In cases where they defined military-unique requirements that could not be restated in performance terms without jeopardizing safety, reliability, or performance, the military specifications and standards were retained.
- Today, the Department of Defense relies on more than 30,000 federal and industry standards, to include performance specifications, international standardization agreements, non-government standards, and commercial item descriptions, as well as defense specifications and standards. In October 2002, the Defense Standardization Executive approved a Joint Materiel Standards Roadmap, developed in response to a June 6, 2001, tasking from the Under Secretary of Defense (Acquisition, Technology, and Logistics). The roadmap defines a course of action to ensure that materiel standards used by the Department of Defense, both commercial and government, continue to support the warfighters' operational requirements for joint Service and coalition interoperability and dramatically reduce the logistics footprint, as articulated in the Force-centered Logistics Enterprise. The objective of the roadmap is to reduce the number of endorsed standards to those required to support these objectives and enable the development of an automated tool to assist Program Managers.
- Because of our success in transforming military specifications and standards and the way that we apply them on contracts, it is no longer required to obtain a waiver from the Milestone Decision Authority to cite military specifications or standards in solicitations and contracts. Elimination of the waiver requirement should not be perceived as a return to the "old way of doing business," where military specifications and standards were often routinely applied to contracts. Every program office should assess requirements and apply only those specifications and standards necessary to define essential needs and manage risk. Program Executive Officers, Program Managers, and others in the acquisition and technical communities should ensure appropriate use of specifications and standards in their programs.
- The Department of Defense will normally use performance specifications (i.e., DoD performance specifications, commercial item descriptions, and performance-based non-Government standards) when purchasing new systems, major modifications, upgrades to current systems, and commercial items for programs in all acquisition categories. The Department of Defense additionally will normally emphasize conversion to performance specifications for the re-procurement of existing systems where supported by a business case analysis; for programs in all acquisition categories.

- If performance specifications are not practicable, or if stating requirements in performance terms is not practicable because of essential interface or interoperability requirements, the Department of Defense may state its needs using prescriptive requirements (i.e. dimensions, materials, etc.).
- The most recent version of MIL-STD-882D, "DoD Standard Practice for System Safety," should be used to manage a program's Environment, Safety, and Occupational Health (ESOH) risks.
- Military specifications and standards contained in contracts and product configuration technical data packages for re-procurement of items already in inventory should:
    - Be streamlined to remove non-value-added management, process, and oversight specifications and standards;
    - When justified as economically beneficial over the remaining product life cycle by a business case analysis, be converted to performance-based acquisition and form, fit, function, and interface specifications to support programs in on-going procurement, future re-procurement, and post-production support.
- The Director, Naval Nuclear Propulsion, determines the specifications and standards for naval nuclear propulsion plants in accordance with 42 U.S.C. 7158 and E.O. 12344.
- DoD Instruction 4120.24 and DoD 4120.24-M contain additional standardization guidance.

The program manager should structure a PBBE to accomplish the following:

- Convey product definition to industry in performance terms;
- Use systems engineering and management practices, including affordability, Integrated Product and Process Development , and support, to fully integrate total Life-cycle considerations;
- Emphasize past performance;
- Motivate process efficiency and effectiveness up and down the entire supplier base-primes, subcontractors and vendors-through the use of contractor-chosen commercial products, practices, and processes;
- Encourage Life-cycle risk management versus risk avoidance;
- Simplify acquisition;
- Transfer acquisition tasks to industry where cost effective, risk-acceptable, and where commercial capabilities exist; and
- Use performance specifications or convert to performance specifications during reprocurement of systems, subsystems, components, spares, and services beyond the initial production contract award; and during post-production support to facilitate technology insertion and modernization of operational weapons systems.

Systems that benefit from a PBBE include highly interoperable systems, high-tech/high-cost systems, high return on investment systems, systems requiring a high degree of logistics readiness and/or technology insertion opportunity, and/or systems with a high total ownership cost and/or a long predicted life.

11.7. Total Life-Cycle Systems Management

Per DoD Directive 5000.01, the Program Manager (PM) is accountable for accomplishing program objectives over the life cycle, including during sustainment. Consequently the PM is responsible for the implementation, management, and/or oversight of activities associated with the system's development, production, fielding, sustainment and disposal. Life-cycle management emphasizes early and continuing emphasis on translating performance objectives into an operationally available and affordable capability over the program life cycle. Key PM responsibilities include:

- Developing and implementing a life-cycle sustainment strategy acquiring an integrated product support package based on achieving key sustainment performance metrics (e.g., materiel availability, materiel reliability, mean down time, ownership costs, footprint, etc.)
- Providing continuous, reliable, affordable support in accordance with performance agreements with force providers.
- Ensuring the system is supported at optimum levels in accordance with performance agreements among government and industry support providers throughout the life cycle.
- Maintaining visibility into cost/capability/risk decisions across the life cycle.

Performance-based life-cycle product support is the strategy program mangers will use in implementing life-cycle management. It is neither contractor logistics support, nor a contracting strategy. It is a performance-oriented strategy arrived at by analyzing alternatives which defines desired logistics support outcomes. Sources of support may be organic, commercial, or a combination thereof. The primary focus is to optimize customer support and system availability at the lowest ownership cost in accordance with statutory requirements. The life-cycle product support strategy provides the framework for acquiring, fielding and supporting a sustainable system throughout the life cycle to deliver the required readiness. It integrates sustainment considerations using outcome based metrics to drive management, design, and logistics decisions and actions. As documented in chapter 5, this includes:

- Establishing a balanced set of sustainment metrics centered around materiel availability
- Impacting the system's design to achieve the sustainment metrics
- Fielding the capability to achieve the sustainment metrics
- Tracking performance against sustainment metrics and accountability for achieving them
- Taking actions (including anticipating performance) to correct performance short comings

During acquisition, the PM's focus is primarily through the acquisition community chain (e.g. the OSD, Service Secretariat, Program Executive Officer chain, etc.) with requirements input from the user and sustainment communities. The focus is to base major decisions on system-wide analyses with the full understanding of the life-cycle consequences of those decisions on system performance and affordability. It includes the:

- Specification of design parameters for sustainment related system performance capabilities.
- Application of systems engineering to determine the right balance between the system's design requirements and the logistics support requirements to sustain the operational capabilities at an affordable price. This includes using supporting sustainment metrics (e.g., Mean Down Time, Logistics Footprint, etc.) as well as enablers (e.g. condition based maintenance, diagnostics, prognostics, corrosion protection/mitigation, etc.) with their associated metrics to achieve the mandatory sustainment metrics.
- Planning for, resourcing, and executing the design, acquisition, management, and fielding of an integrated product support package to sustain the maintenance and support concepts to meet the materiel availability requirements.

During the operations phase the PM's focus is primarily through the user (e.g. the force providers, type commander) and sustainment communities (e.g., depots, industrial base, supply, transportation, and other logistics organizations) with support from the acquisition community. The focus is on supporting the user's ability to effectively meet mission requirements with the application of continuous process improvement principles. This involves monitoring performance to identify major readiness degraders (e.g., reliability, cycle time, cost, etc.) and to:

- Align and refine the product support package (e.g., the logistics elements) and sustainment processes to achieve the sustainment metrics
- Engage the various communities to achieve optimum materiel readiness
- Optimize or reduce the logistics demand (including the logistics footprint) and support processes (e.g., training, technical data, supply chain, maintenance, etc.) based on actual conditions
- Reduce total ownership costs
- Identify and implement design changes to address evolving requirements, technology obsolescence, diminishing manufacturing sources, or materiel availability shortfalls.

System sustainment is enabled by effective planning, development, implementation, and management. To accomplish this, the program manager needs to adequately plan for the long-term supportability and sustainment through the aggressive application of performance-based life-cycle product support strategies. The plan for implementing these strategies seamlessly spans the entire life cycle and is spelled out in the Life-Cycle Sustainment Plan (LCSP). See section 5.1.2.2 for additional information and section 5.4 for specific LCSP focus areas in each life-cycle phase.

11.8. Integrated Product and Process Development (IPPD)

IPPD is the DoD management technique that simultaneously integrates all essential acquisition activities through the use of multidisciplinary teams to optimize design, manufacturing, and supportability processes. One of the key IPPD tenets is multidisciplinary teamwork through Integrated Product Teams.

IPPD facilitates meeting cost and performance objectives from product concept through production, including field support. The 10 tenets of IPPD can be summarized into the following 5 principles:

- Customer Focus
- Concurrent Development of Products and Processes
- Early and Continuous Life-Cycle Planning
- Proactive Identification and Management of Risk
- Maximum Flexibility for Optimization and Use of Contractor Approaches

11.9. Technical Representatives at Contractor Facilities

Program managers should maximize the use of Defense Contract Management Agency (DCMA) personnel at contractor facilities. Program managers and DCMA Contract Management Offices should jointly develop and approve program support plans for all Acquisition Category I program contracts to ensure agreement on contract oversight needs and perspectives.

The program manager should only assign technical representatives to a contractor's facility as necessary, and as agreed to by the Director, DCMA. A Memorandum of Agreement should specify the duties of the technical representative and establish coordination and communication activities. Technical representatives shall not perform contract administration duties as outlined in Federal Acquisition Regulation (FAR) Section 42.302(a).

11.10. Contractor Councils

The Defense Contract Management Agency (DCMA) supports the formation of management, sector, and/or corporate councils by each prime contractor under DCMA cognizance that provide Acquisition Category (ACAT) I, ACAT IA, or ACAT II program support. These councils provide an interface with the Contract Management Office Commander; the Defense Contract Audit Agency Resident Auditor; representatives from all affected acquisition management activities (including program managers, Item Managers, and Standard Procurement System Component Team Leaders), or designated representatives for any of the above listed individuals. Acquisition managers or designees should support both council activities and council-sponsored Working-Level Integrated Product Teams. Acquisition managers should assist the councils and keep all the stakeholders informed about issues affecting multiple acquisition programs, work issues quickly, and elevate unresolved issues to appropriate levels for resolution. These councils may identify and propose acquisition process streamlining improvements. Acquisition managers should assist and encourage councils to coordinate and integrate program audit and review activity, support and promote civil-military integration initiatives, and accept contractor Standard Procurement System proposals and other ideas that reduce total ownership cost while meeting performance-based specifications.

The program office staff should interface with contractors' councils, keeping in mind that such councils are not federal advisory committees under the Federal Advisory Committee Act. The staff may find that these councils strengthen the corporate relationship with the Department of Defense, provide an interface between company representatives and acquisition managers, communicate acquisition reform initiatives, or even resolve issues. In leading corporate endeavors, such as Standard Procurement System proposals, civil-military integration ideas, or other initiatives designed to achieve efficiencies for the company, these councils may ultimately produce savings for the Government.

11.11. Government Property

11.11.1. Government Property in the Possession of Contractors (GPPC)

All program managers should prevent the unnecessary furnishing of Government Property. The program manager should assign GPPC management authority within the program office, and identify needed actions, reviews, and reports. Decisions about acquisition, retention, disposition, and delivery requirements should be well informed and timely. GPPC no longer needed for current contract performance or future needs should be promptly disposed of or reutilized in accordance with applicable laws and regulations; or stored under a funded storage agreement. The program manager should document decisions regarding GPPC in the contract file.

GPPC includes Government property that is not "owned" by the program manager, but is "used" on the program. Government property may only be furnished to contractors under the criteria, restriction, and documentation requirements addressed in Federal Acquisition Regulation 45.3.

11.11.2. Contractor Acquired Property

Contractor acquired property is property acquired, fabricated, or otherwise provided by the contractor for performing a contract and to which the Government has title.

DoD policies, processes, and practices are structured on delivery, receipt and acceptance of property. This aligns and is consistent with other DoD processes and practices (e.g., Wide-Area Work Flow, Unique Item identification). Although the DoD may have title to some property, e.g., property acquired, fabricated, or otherwise provided by the contractor for performing a contract, such property has not yet been delivered.

Upon delivery to the Government, contractor acquired property should be recorded in the appropriate property accountability system. If this property is subsequently provided to a contractor for follow-on contracts, it will be managed as government furnished property. Consistent with DoD Instruction 5000.64, there is no requirement for accountability by DoD Components for such property prior to delivery to the Government. Third parties (to include contractors) have stewardship responsibility, to include creating and maintaining records of all Government property accountable to the contract, consistent with the terms and conditions of the contract or third party agreement, for the Government property in their care.

11.11.3. Government Furnished Property

"Government-furnished property" means property in the possession of, or directly acquired by, the Government and subsequently furnished to the contractor for performance of a contract.

Although the Department of Defense may not have physical custody, to maintain effective property accountability and control and for financial reporting purposes, DoD Components are required to establish records and maintain accountability for property (of any value) furnished to contractors as Government Furnished Property.

11.12. Integrated Digital Environment (IDE)

DoD policy requires the maximum use of digital operations throughout the system life cycle. The program IDE is part of the larger DoD IDE. It should keep pace with evolving automation technologies and provide ready access to anyone with a need-to-know, as determined by the program manager.

Program managers should establish a data management system within the IDE that allows every activity involved with the program to cost-effectively create, store, access, manipulate, and exchange digital data. This includes, at minimum, the data management needs of the system engineering process, modeling and simulation activities, test and evaluation strategy, support strategy, and other periodic reporting requirements.

Industry partners have been strongly encouraged to develop and implement IDE solutions that best meet the needs of their preferred business model. The program IDE should take maximum advantage of and have minimum impact on existing industry solutions. Solicitations should require IDE proposals to support system life-cycle activities. Unless analysis verifies prohibitive cost or time delays, or a potential compromise of national security, new contracts should require the contractor to provide on-line access to programmatic and technical data. Contracts should give preference to on-line access (versus data exchange) through a contractor information service or existing IT infrastructure. While contracts should minimally specify the required functionality and data standards, the data formats of independent standards-setting organizations should take precedence. The issue of data formats and transaction sets should be independent of the method of access or delivery.

The program manager should use existing infrastructure (e.g., Internet or wireless LANs) when practicable.

The program manager should address the status and effectiveness of the IDE at milestone reviews and at other appropriate decision points and/or program reviews.

11.13. Simulation-Based Acquisition (SBA) and Modeling and Simulation (M&S)

SBA is the robust and interactive use of M&S throughout the product life cycle. The program manager should employ SBA and M&S during system design, test and evaluation, and modification and upgrade. The program manager should collaborate with operational users and consider industry inputs during SBA/M&S program planning. Planning should include the application, support, documentation, and reuse of M&S; and the integration of SBA/M&S across functional disciplines.

The following additional considerations are useful during SBA/M&S planning activities:

- Plan for SBA/M&S and make necessary investments early in the acquisition life cycle.
- Use verified, validated, and accredited models and simulations, and ensure credible applicability for each proposed use.
- Use data from system testing during development to validate the use of M&S.
- Use SBA/M&S to supports efficient test planning, pre-test results prediction, and the validation of system interoperability; and supplement design qualification, actual test and evaluation, manufacturing, and operational support;
- Involve the operational test agency in SBA/M&S planning to support both developmental test and operational test objectives.
- Have the Defense Intelligence Agency review and validate threat-related elements.

11.14. Independent Expert Review of Software-Intensive Programs

The program manager for an Acquisition Category (ACAT) ID or IC program that requires software development to achieve the needed capability should convene an independent expert program review after Milestone B and prior to the system Critical Design Review. The program manager, or other acquisition official in the program chain of command up to the DoD Component Acquisition Executive, should also consider independent expert program reviews for ACAT IA, II, and III programs. The independent expert review team should report review findings directly to the program manager.