MANUAL FOR THE OPERATION OF THE JOINT CAPABILITIES INTEGRATION AND DEVELOPMENT SYSTEM

J-8

DISTRIBUTION: A, B, C, S

References: See Enclosure E for References.

This manual is not intended to stand alone – readers are strongly encouraged to become familiar with the Joint Requirements Oversight Council (JROC) Charter and JCIDS Instruction, Reference [1] **before reviewing this manual.**

1. Purpose: This manual provides procedural guidance for the Joint Capabilities Integration and Development System (JCIDS) which is established as the primary means for the JROC to fulfill its statutory responsibilities to the Chairman of the Joint Chiefs of Staff (CJCS) as outlined in Reference [2]. These responsibilities include assessing joint military capabilities, and identifying, approving, and prioritizing gaps in these capabilities, to meet applicable requirements in the National Defense Strategy (NDS). It provides detailed guidelines and procedures for JCIDS to facilitate robust capability requirements portfolio management and the timely and cost-effective development of capability solutions for the warfighter. Exceptions to the rules are accepted on a case by case basis and it is understood that each capability requirement is unique and may require waivers to meet its needs.

1.1. Enclosure A outlines the deliberate, urgent, and emergent capability requirements process used under JCIDS. Each appendix provides guidance on development and staffing. Additionally, it includes appendices for gatekeeping and staffing metrics.

1.2. Enclosure B outlines the formats for JCIDS documents. These include the Initial Capabilities Document (ICD), Information Systems ICD (IS-ICD), Capability Development Document (CDD), Information Systems CDD (IS-CDD), Joint Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTmLPF-P) Change Recommendation (DCR), Joint Urgent Operational Need (JUON), and Joint Emergent Operational Need (JEON). Additionally, it includes appendices for the development of performance and system attributes and for the DoD Architecture Framework (DoDAF) primer for JCIDS.

1.3. Enclosure C outlines the capability requirements portfolio management process and includes appendixes for the Capability Gap Assessment (CGA) and identification of joint military capability requirements.

1.4. Enclosure D provides an overview of the Requirements Management Certification Training (RMCT).

2. Superseded/Cancellation.

2.1. The JCIDS Manual, 12 February 2015, "Manual for the Operation of the Joint Capabilities Integration and Development System," including errata as of 18 December 2015, is hereby superseded.

3. Applicability. This manual applies to the Joint Staff, Services, Combatant Commands (CCMDs), Combat Support Agencies, and other Department of Defense (DoD) Agencies.

4. Procedures. Provides procedural guidance for JCIDS and other requirements-related processes and activities.

4.1. The JROC is implemented by the rules established in its charter to satisfy the statutory responsibilities under Title 10, U.S.C. § 181. Reference [1] outlines the structure of the JROC's subordinate boards, and identifies organizations involved in JROC activities.

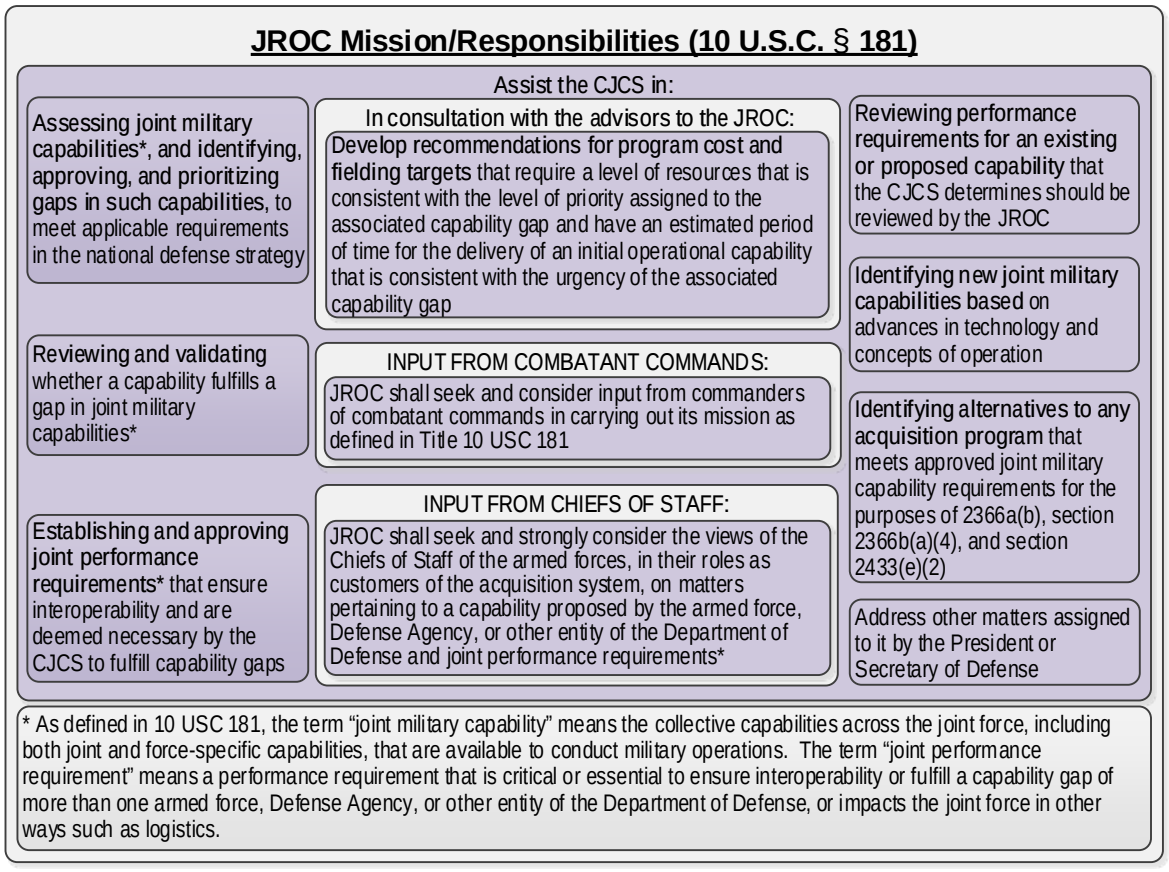

Figure 1: JROC Mission/Responsibilities (Title 10 U.S.C. § 1818)

4.1.1. A detailed description of JCIDS is organized into logical subsections shown in Figure 2.

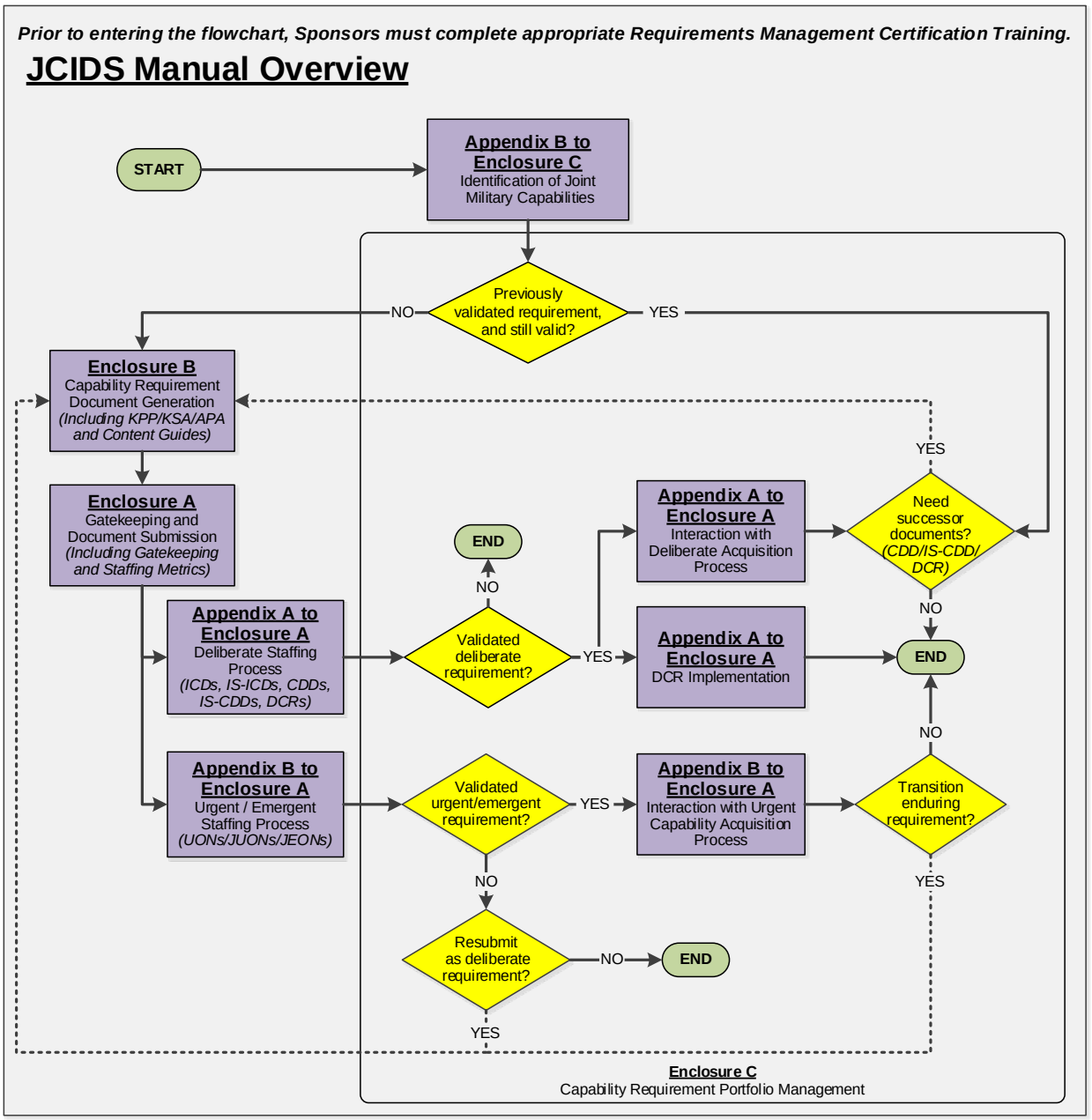

Figure 2: JCIDS Manual Overview

4.1.2. In addition, Reference [3] provides Uniform Resource Locators (URLs) for the JCIDS Wiki sites, which provides up to date information on JCIDS guidance and implementation.

4.2. Document Staffing and Validation: Enclosure A outlines the staffing and gatekeeping process for all incoming capability requirements documents prior to deliberate or expedited staffing and validation.

4.2.1. Appendix A to Enclosure A outlines the deliberate staffing process used for the review and validation of capability requirements, including the associated capability gaps, and proposed materiel and/or non-materiel capability solutions.

4.2.2. Appendix B to Enclosure A outlines the urgent/emergent staffing process for expedited review and validation of urgent or emergent capability requirements, and associated capability gaps, which if unmitigated would result in unacceptable loss of life or critical mission failure in ongoing or anticipated contingency operations.

4.3. Capability Requirements Document Generation: Enclosure B outlines the format for capability requirements documents. Sponsors use these documents to articulate joint military capability requirements, associated capability gaps, and other related data and to provide refined capability requirements and system-level performance attributes for materiel and non-materiel capability solutions. This enclosure also includes detailed content, certification, and endorsement guides.

4.4. Capability requirements Portfolio Management: Enclosure C provides detail on activities performed by the Functional Capability Boards (FCBs) and other stakeholders to accomplish capability requirements portfolio management. Figure C-2, an outline of the Capability-Mission Lattice (CML), is provided as an integrating construct for identification of capability requirements and maintaining traceability to strategic guidance, missions of the joint force, Service and Joint Concepts, Concept of Operations (CONOPS), and other DoD activities.

4.5. Capability requirements Identification: Enclosure C outlines the various processes which Sponsors use to identify their capability requirements, associated capability gaps, and proposed materiel and non-materiel capability solutions for submission into JCIDS for review and validation. Enclosure C also includes discussion of Capabilities-Based Assessments (CBAs).

4.6. Requests for exceptions or variances to this manual or the document formats and processes must be directed to the Joint Staff Gatekeeper.

4.6.1. The Joint Staff Gatekeeper will work in coordination with the document Sponsor and the appropriate FCB(s) to ensure any exceptions or variances meet the needs of the validation authority while allowing for appropriate flexibility in the capability requirements process.

4.6.2. Waivers granted by the Joint Staff Gatekeeper shall be documented in memorandum format and attached to associated documents in Knowledge Management and Decision Support (KM/DS) to provide traceability for future staffing and validation activities. At the discretion of the Joint Staff Gatekeeper, waivers may be documented by KM/DS note in lieu of a hard copy memorandum.

5. Summary of Changes. This updated manual:

5.1. Includes significant changes from the previous version; primary stakeholders should review it in its entirety.

5.2. Incorporates changes to the Chairman's functions. This includes the capability requirements process and associated roles and responsibilities of the JROC, its subordinate boards, and other supporting organizations resulting from the Fiscal Year 2017 and 2018 National Defense Authorization Act (FY17 and FY18 NDAAs).

5.3. Restructures the manual into a formatted document with five Enclosures to support primary stakeholder use. See Figure 2 for an overview of this manual.

5.4. Focuses on joint military capabilities and capability gaps per the revised Title 10 U.S.C. § 181.

5.4.1. Implements guidelines and procedures for establishing and approving Joint Performance Requirements (JPRs).

5.4.1.1. [Appendix C to Enclosure A, Page A-C-6, Paragraph 3.2.2.] How JPRs are designated and the staffing process.

5.4.1.2. [Appendix C to Enclosure A, Page A-C-9, Figure A-16] Depicts Certification and Endorsement Responsibilities including those requirements designated as JPRs.

5.4.1.3. [Appendix C to Enclosure B, Page B-C-11, Paragraph 2.5.5.5.1. and Figure B-6] Explains how JPRs are identified in capability requirements documents.

5.4.2. Adds guidance to address joint interoperability.

5.4.2.1. [Appendix C to Enclosure B, Page B-C-13, Paragraph 2.5.7.] Adds section to the CDD for joint interoperability that specifies how the individual system will interoperate within the joint environment including physical or net-ready interoperability effects on joint operations or operations with allies and partners.

5.4.2.2. [Appendix C to Enclosure B, Page B-C-7, Paragraph 2.5.4.3. and Page B-C-13, Paragraph 2.5.7.1.] Includes guidance on how a Sponsor can address Modular Open System Approach (MOSA) in the Program Summary section and the Joint Interoperability section of the CDD in accordance with (IAW) Title 10 U.S.C. § 2446b.

5.5. Delegates authorities where appropriate to support a more streamlined and responsive system.

5.5.1. [Appendix C to Enclosure A, Pages A-C-7 and A-C-8, Paragraph 3.2.3.6.] Reduces Joint Staffing Designators (JSDs) to JROC-Interest, JCB-Interest, and Joint Information. Deletes Joint Integration.

5.5.2. [Appendix C to Enclosure A, Page A-C-8, Paragraph 3.2.3.6.1.] Deletes requirement for all Acquisition Category (ACAT) I programs to automatically be

given a JSD of JROC Interest. JROC no longer tied directly to cost, but instead tied to joint equities as defined under the JPRs in Title 10 U.S.C. § 181.

5.5.3. [Appendix C to Enclosure A, Page A-C-9, Figure A-16] Delegates Certifications/Endorsements to the Sponsor unless joint interoperability is clear or there are multi-service equities.

5.5.4. Reduces the number of "Mandatory" Key Performance Parameters (KPPs) to the four statutory mandatory KPPs (Energy, System Survivability, Force Protection, and Sustainment).

5.5.4.1. [Appendix C to Enclosure B, Page B-C-10, Paragraph 2.5.5.4.] Reduces number of mandatory KPPs under Section 5 of the CDD, and therefore no longer requiring that Net-Ready or Training be mandatory KPPs. Note: Net-Ready still required but can be addressed as a KPP, KSA, or APA.

5.5.4.2. [Appendix D to Enclosure B, Page B-D-5, Paragraph 2.5.5.2.] Reduces number of mandatory KPPs under Section 5 of the Information Systems-CDD, and therefore no longer requiring that Net-Ready or Training be mandatory KPPs. Note: Net-Ready still required but can be addressed as a KPP, KSA, or APA.

5.5.4.3. [Appendix G to Enclosure B, Page B-G-2, Paragraph 3.] Provides guidance for mandatory performance attributes.

5.6. Minimizes touch points between Sponsor and the JROC.

5.6.1. Reduces the number of mandatory capability requirements documents.

5.6.1.1. [Appendix A to Enclosure A, Page A-A-17, Paragraph 2.6.1.4. and Appendix C to Enclosure B, Page B-C-1, Paragraph 1.1.2.] Capability Production Document (CPD) no longer required. Sponsors can update a validated CDD and provide a CDD Update to the validation authority for any changes that are deemed significant.

5.7. Addresses evolutionary acquisitions.

5.7.1. Provides options for the Sponsor to address the evolving threat informed by military risk and the maturity of the technologies available.

5.7.1.1. Evolving threat and phased capability development supported by guidance within the ICD [Appendix A to Enclosure B, Page B-A-4, Paragraph 2.5.2.4. and Page B-A-8, Paragraph 2.5.3.6.1.] and within the CDD [Appendix C to Enclosure B, Page B-C-4, Paragraph 2.5.2.3. as well as Appendix C to Enclosure B, Page B-C-9, Paragraph 2.5.5.1.2. and Paragraph 2.5.5.2. and supporting paragraphs].

5.7.1.2. [Appendix C to Enclosure B, Page B-C-7, Paragraph 2.5.4.3. and Page B-C-13, Paragraph 2.5.7.1.] Provides guidance within the Joint Interoperability section of the CDD including MOSA to support an incremental approach.

5.7.2. Adds Incremental CDD option for Sponsors to address an incremental or Family of Systems (FoS) approach.

5.7.2.1. [Appendix A to Enclosure A, Page A-A-18, Paragraph 2.6.2. and Figure A-7] Provides guidance to Sponsors for how an incremental CDD approach would interact with acquisitions.

5.7.2.2. [Annex A to Appendix C to Enclosure B, Page B-C-A-1] Explains the document format for an incremental or FoS CDD wherein the Sponsor can provide annexes either all at once or over time.

5.8. Addresses the concern with identifying intelligence supportability requirements and enhancing survivability requirements early in the process to enable selection of capabilities that meet operational requirements.

5.8.1. [Annex G to Appendix G to Enclosure B]. Updates the Intelligence Supportability Guide and includes new guidance on Intelligence Supportability, Critical Intelligence Parameter (CIP) Breach, Intelligence Mission Data, Interoperability and Foreign Intelligence, and Counterintelligence.

5.8.2. [Appendix A to Enclosure B, Page B-A-4, Paragraph 2.5.2. and Page B-A-7, Paragraph 2.5.3.4] Updates the Threat Summary section and Capabilities Requirements and Gaps Overlaps section of the ICD including new information on threat assessment, CIP breach, and intelligence supportability.

5.8.3. [Appendix A to Enclosure A, Page A-A-33, Figure A-12 and Page A-A-34 and A-A-35, Paragraphs 3.4.5.1. and 3.4.5.2.] Updates information on CIP breaches including an up-front assessment conducted by the Lead FCB to determine if other programs or systems are affected.

5.8.4. [Annex C to Appendix G to Enclosure B] Updates the System Survivability Guide including adding information regarding kinetic, Electromagnetic Spectrum (EMS), and cyber survivability and linkages to guidebooks for each of the three areas.

5.8.5. [Appendix A to Enclosure B, Page B-A-7, Paragraph 2.5.3.5.] Updates the Capabilities Requirements and Gaps Overlaps section of the ICD including early identification of criteria used to determine the Cyber Survivability Risk Category (CSRC) and EMS Survivability Risk Category.

5.9. [Appendix A to Enclosure A, Page A-A-34, Paragraph 3.4.3. and Page A-A-33, Figure A-12]. Adds Classified Information Compromise Assessment (CICA) section to ensure capability development addresses future compromises due to insider threat.

5.10. Adds guidance on JROC support to the Secretary of Defense's (SecDef's) Investment Review Process in developing recommendations for program cost and fielding targets pursuant to Title 10 U.S.C. § 2448a. (Title 10 U.S.C. § 181).

5.10.1. [Appendix A to Enclosure A, Page A-A-14, Paragraph 2.6.1.2.2. and Page A-C-14, Paragraph 3.4.2.5.] Describes how the JROC will leverage the post-analysis of alternatives (AoA) review to provide recommendations to the Investment Review Process for program cost and fielding targets.

5.10.2. Separate policy is being developed for the Investment Review Process.

6. Releasability. UNRESTRICTED. This directive is approved for public release; distribution is unlimited on NIPRNET.

7. Effective Date. This INSTRUCTION is effective 90 days after receipt.

ANTHONY R. IERARDI
LTG, USA
Director, J-8, Joint Staff

Enclosures
- A - JCIDS
- B - JCIDS Document Formats
- C - Capability Requirements Portfolio Management
- D - Requirements Management Certification Training
- E - References
- GL- Glossary

TABLE OF CONTENTS

Page

TABLE OF FIGURES

(INTENTIONALLY BLANK)

ENCLOSURE A
JCIDS

1. Overview.

1.1. Purpose. The purpose of JCIDS is to enable the JROC to execute its statutory duties to assess joint military capabilities, and identify, approve, and prioritize gaps in these capabilities, to meet applicable requirements in the NDS as specified in Reference [2]. JCIDS staffing lanes depend upon the timelines of the operational requirement, as shown in Figure A-1. These timelines can be further tailored on a case-by-case basis upon agreement by the Joint Staff Gatekeeper or the validation authority.

1.2. Applicability. This enclosure applies to the Joint Staff, Services, CCMDs, Combat Support Agencies, and other Department of Defense (DoD) Components.

1.3. Proponent. The proponent for this enclosure is the J-8/Joint Capabilities Division (JCD). For questions, contact J-8/JCD at (703) 695-2705.

2. Introduction to JCIDS.

2.1. JCIDS starts with a robust assessment of missions, functions, and tasks in the context of threat and environment, to identify and quantify capability requirements. Capability requirements are measures of effectiveness (MOE) in the form of mission focused task statements that are best written in "task, condition and standard" format. Capability requirements are service, solution, and cost agnostic, and are thought of as "what needs to be done (the metric), and to what level (the initial value)."

2.2. Identified capability requirements are then compared with the existing and programmed capability solutions across the joint force to identify potential capability gaps. Capability gaps which represent unacceptable risk may require new or modified materiel or non-materiel capability solutions, and the application of resources. The level of risk and the timeliness of the threat will drive the sponsor to the appropriate documentation and validation process.

2.3. The content is captured to initial documentation that will include traceability to the source of the capability requirements, the identification of capability gaps, assessment of associated risk, and timeliness of capability solution needed by the warfighter.

2.4. An AoA or other assessment is performed to assess a range of possible Alternatives and recommend preferred capability solution approaches for informed decision making.

2.5. Following the decision on the best path forward for the capability solution, the key aspects of follow-on documentation will include traceability to validated capability requirements, measures of performance (MOP), and required

resourcing to develop the proposed capability solutions(s). This follow-on documentation will inform technology maturation and/or acquisition programs for associated solutions.

2.6. In order for any these documents to become actionable, they must be validated by the appropriate validation authority. The process for validating documents can address a wide spectrum of timeliness regarding warfighter needs, from near to long term.

3. JCIDS Process Lanes.

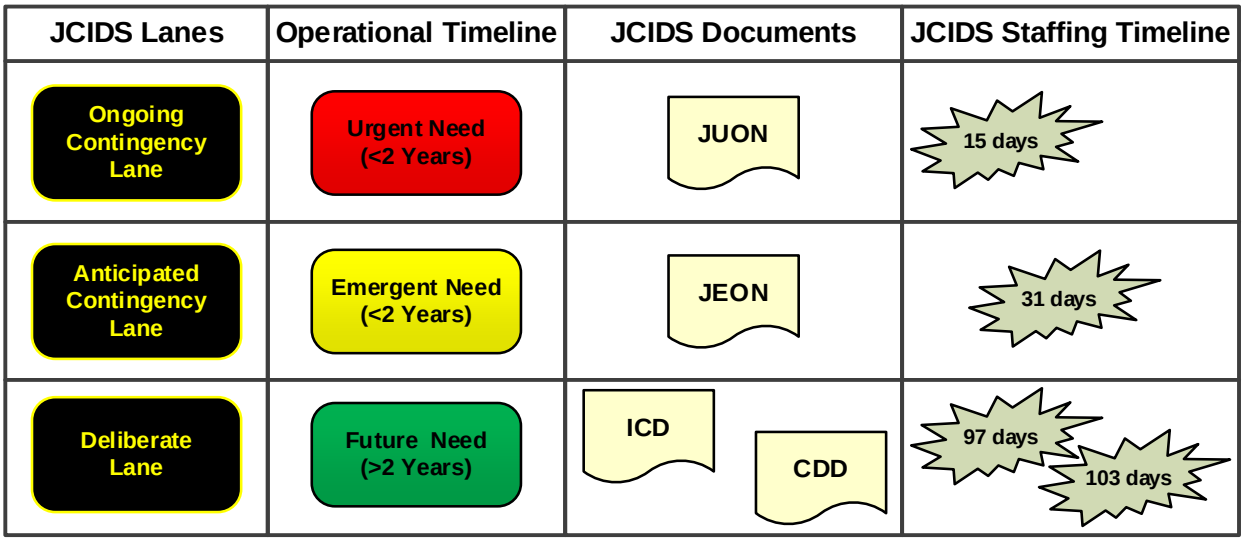

Figure A- 1: JCIDS Process Lanes

3.1. JCIDS Deliberate Process. The deliberate process is for future needs (>2 years) and uses the ICD to validate joint military capability requirements and the CDD to validate proposed capability solutions. The staffing for documents in the deliberate lane is 97 days for an ICD (or IS-ICD variant) and 103 days for a CDD (or IS-CDD variant) after the document is submitted in JCIDS for staffing and further consideration by the Joint Staff Gatekeeper. Appendix A to this enclosure provides additional detail on the JCIDS Deliberate Process.

3.2. JCIDS Urgent/Emergent Process. The urgent and emergent process lane provides Sponsors with the ability to address capability gaps in ongoing or anticipated contingency operations as expeditiously as possible within the 2-year timeframe. The JUON or JEON provide the required documentation to approve joint military capability requirements for this lane. The staffing timeline for urgent and emergent needs is conducted as expeditiously as possible within 15 and 31 days respectively. Appendix B to this enclosure provides additional details on the JCIDS Urgent and Emergent processes.

3.3. Types of capability requirements documents. The four categories of capability requirements documents are:

3.3.1. ICD (included the IS-ICD variant). An ICD specifies one or more capability requirements and associated capability gaps that represent

unacceptable operational risk if left unmitigated. The ICD also recommends partially or wholly mitigating identified capability gap(s) with a materiel capability solution, or some combination of materiel and non-materiel solutions. A validated ICD is an entrance criterion necessary for each Materiel Development Decision (MDD).

3.3.2. DCR. A DCR recommends partially or wholly mitigating one or more capability gaps with non-materiel capability solutions, through changes to one or more of the eight DOTmLPF-P areas. In cases where a DCR is not generated as a successor document to a validated ICD, it also specifies the capability requirements and associated capability gaps for review and validation.

3.3.3. CDD (includes the IS-CDD variant). A CDD specifies capability requirements, in terms of system level performance attributes which include Key Performance Parameters (KPPs), Key System Attributes (KSAs), and Additional Performance Attributes (APAs) to support development of one or more increments of a materiel capability solution. A validated CDD is a requirement for the Development Request for Proposal (RFP) release decision point before Milestone B. In cases where the Milestone Decision Authority (MDA) waives Milestone A or B but an Engineering and Manufacturing Development (EMD) phase of acquisition will be conducted, the CDD shall be validated before RFP release for the EMD phase of acquisition or the beginning of the EMD phase of acquisition, whichever comes first. In cases where Milestone B and C are combined, such as for high cost first articles of spacecraft and ships, the CDD shall be the authoritative document for the first article produced during EMD without the need for updated CDDs.

3.3.4. JUON, JEON, and DoD Component UON. A JUON, JEON, or DoD Component UON specifies capability requirements driven by ongoing or anticipated contingency operations, which if left unfulfilled, would result in capability gaps leading to unacceptable loss of life or critical mission failure. Expedited staffing and validation procedures for JUONs and JEONs are outlined in this manual. A validated JUON, JEON, or DoD Component UON, or other validated capability requirement, is necessary to initiate urgent capability acquisition efforts unless the Secretary of Defense or Deputy Secretary of Defense determines that a documented deficiency requires the use of their Rapid Acquisition Authority IAW Section 806(c) of Public Law 107-314.

APPENDIX A TO ENCLOSURE A
JCIDS DELIBERATE PROCESS

1. Overview.

1.1. Purpose. The deliberate JCIDS process serves as a means for Sponsors to submit for review and approval any new or modified joint military capability requirements and associated capability gaps. Additionally, the deliberate process provides the means to validate whether the proposed capability solutions meet approved joint military capability requirements.

1.1.1. Capability requirements documents and their associated validation memorandums serve as the enduring artifacts to identify exactly what requirements were validated, support capability requirements portfolio management, enable acquisition of capability solutions, and inform many other processes and activities across DoD.

1.1.2. All capability requirements documents are drafted based on guidance and the formats in this manual and are provided to the Joint Staff Gatekeeper for initial screening and review before submission for staffing.

1.1.3. Capability requirements documents are then staffed for review and validation by the appropriate requirement validation authority via the processes outlined in this enclosure.

1.1.4. All validated capability requirements documents are archived in the KM/DS system at the URL in Reference [4]. This includes those that are validated by independent validation authorities and updates to validated capability requirements documents. The validated capability requirements documents in KM/DS serve as the basis for development of individual materiel and non-materiel capability solutions.

1.2. Applicability. This Appendix applies to the Joint Staff, Services, CCMDs, and other DoD Agencies.

1.3. Proponent. The proponent for this appendix is the J-8/JCD. For questions, contact J-8/JCD at (703) 695-2705.

2. JCIDS Deliberate Process.

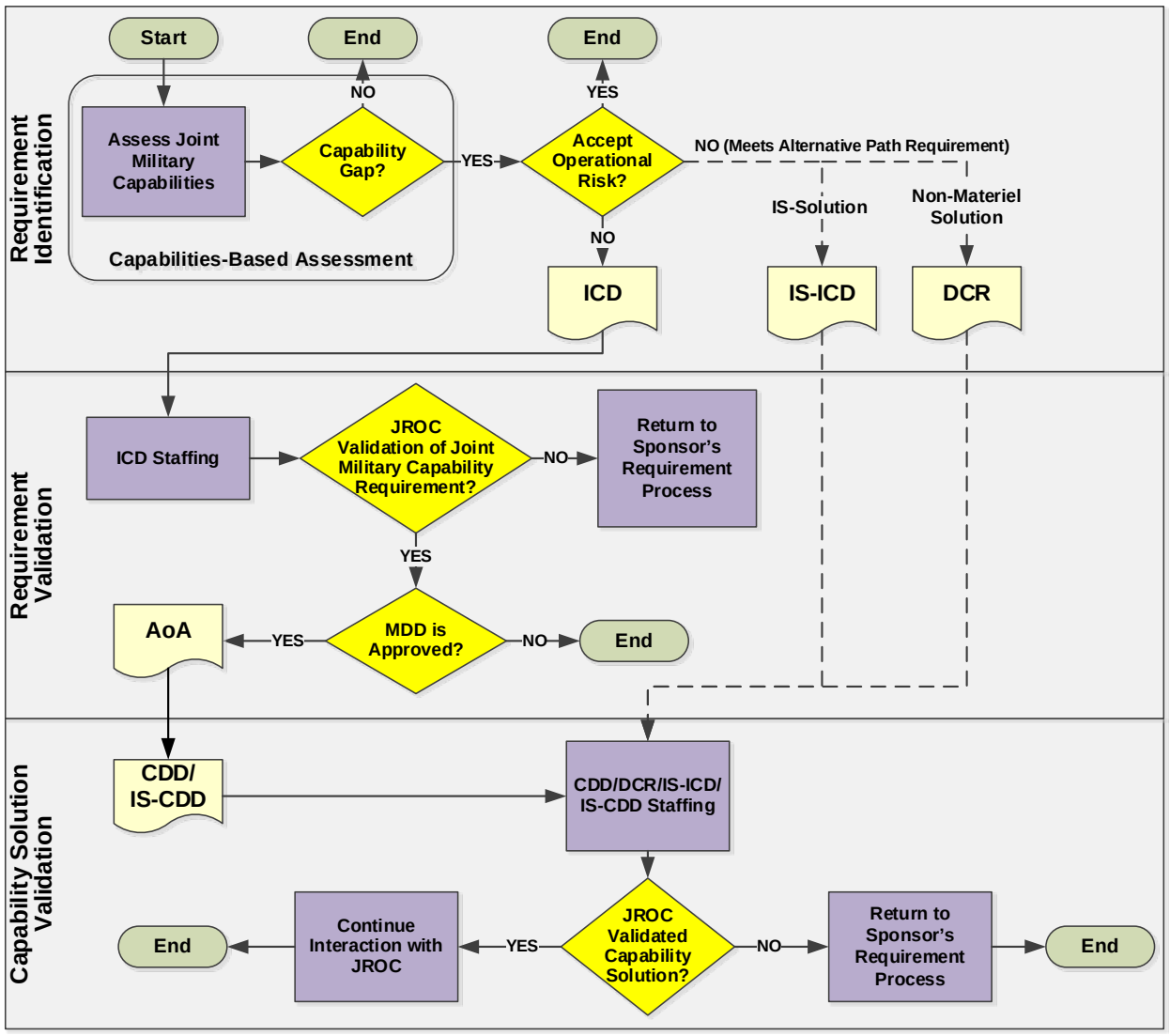

Figure A- 2: JCIDS Process Overview

2.1. Joint military capability requirement (ICD) and capability solution (CDD or Joint DCR) validation. See paragraph 2.5 of this appendix for more information on IS systems (IS-ICD and IS-CDD).

2.1.1. The ICD validation identifies the joint military capability requirements and enables the JROC to perform their statutory duties to assess joint military capabilities and identify, approve, and prioritize gaps in such capabilities.

2.1.1.1. In validating an ICD, the validation authority:

2.1.1.1.1. Validates the capability requirements (and associated initial objective values) as being necessary to fulfill joint military capabilities in support of the national defense strategy and approves prioritization of associated capability gaps.

2.1.1.1.2. Approves the document and supporting data contained therein, including the recommended approach(es) to address the validated capability requirements and eliminate or mitigate, to the maximum extent possible, the capability gaps.

2.1.1.1.3. Includes, where applicable, recommendations for development of the AoA guidance, in support of Reference [5].

2.1.2. The CDD and Joint DCR validation enables the JROC to perform their statutory duties to review and validate whether a proposed capability solution fulfills a capability gap(s) and meets the approved joint military capability requirements established in the ICD(s).

2.1.2.1. In validating a CDD, the validation authority:

2.1.2.1.1. Validates the proposed capability solution fulfills a gap in joint military capabilities or is otherwise necessary to meet applicable requirements in the national defense strategy.

2.1.2.1.2. Approves the document and supporting data contained therein, including the performance attributes (KPPs, KSAs, and APAs, and associated threshold and objective values), and the designation of performance attributes as JPRs where applicable.

2.1.2.1.3. Assesses the risks in meeting those performance attributes in terms of lifecycle cost, schedule, and technological maturity.

2.1.2.1.4. Assesses the affordability of the system as compared to the capability solution being delivered and may consider other alternatives to the proposed solution.

2.1.2.1.5. Approves schedule (Initial Operational Capability (IOC) and Full Operational Capability (FOC)) and procurement quantities.

2.1.2.2. In validating a Joint DCR, the validation authority:

2.1.2.2.1. Validates the proposed capability solution(s) (non-materiel) fulfills a gap in joint military capabilities or is otherwise necessary to meet applicable requirements in the national defense strategy.

2.1.2.2.2. Approves the document and supporting data contained therein, including the change recommendations and implementation plans.

2.1.2.2.3. Assigns the Office of Primary Responsibility (OPR) to accomplish each action listed in the implementation plan.

2.2. Document Sequences. Capability requirements document sequences do not have to follow a purely linear progression as shown in Figure A-2 and may follow variations as outlined in Figure A-3. The ICD is the most common starting point to document capability requirements when a materiel approach is deemed appropriate.

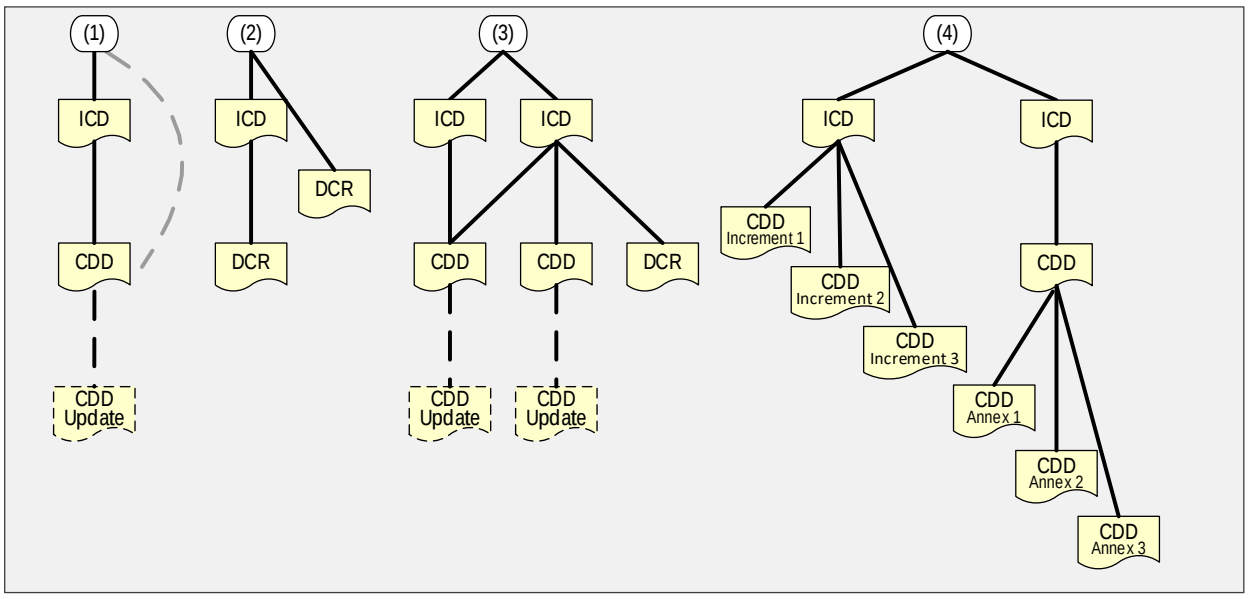

Figure A- 3: Capability Requirements Document Sequences

2.2.1. The ICD typically leads to an AoA or similar study and then the CDD for development of a materiel capability solution. For situations where a system of system-based solution may be appropriate, systems engineering work may be required before proceeding to the AoA study phase. In many cases, a combination of materiel and non-materiel approaches may result from an ICD.

2.2.1.1. A CDD may be generated without an associated ICD, when the Joint Staff Gatekeeper, in coordination with the validation authority and the MDA, approves an ICD waiver.

2.2.1.1.1. This approach may be appropriate when there has already been demonstration of the capability solution in an operational environment. For example, ICDs may not be required when successful JUONs, JEONs, or DoD Component UONs are proposed as enduring capability requirements, or when successful Joint Capability Technology Demonstrations (JCTDs) or experiments with a positive assessment of operational utility are recommended to transition to Program of Records (PORs).

2.2.1.1.2. In cases where the Sponsor proposes to proceed directly to a CDD, the Sponsor will request an ICD waiver through the Joint Staff Gatekeeper IAW Appendix C of this enclosure. The Joint Staff Gatekeeper, in coordination with the MDA and validation authority, may approve the waiver, to be included in the front of the CDD. The MDA may then direct in the MDD that the Materiel Solution Analysis (MSA) phase be abbreviated or eliminated, and further development of a capability solution start directly at Milestone A, B, or C.

2.2.1.1.2.1. The Sponsor will provide ICD content, including capability requirements and capability gap table, in the appropriate successor document as outlined in the Joint DCR and CDD document formats.

2.2.1.1.2.2. The Sponsor will also provide the required architecture views using the Department of Defense Architecture Framework (DoDAF) applicable to the ICD/IS-ICD, in addition to those required for the CDD/IS-CDD, IAW Figure A-4.

2.2.2. Joint DCRs may be generated to document capability requirements when a non-materiel approach is deemed most appropriate.

2.2.2.1. A Joint DCR may be generated from one or more validated ICDs as a non-materiel solution to validated capability requirements and associated capability gaps, or as a complement to a materiel capability solution, which will be developed through the acquisition process. The Joint DCR will provide traceability to the applicable ICD(s). Additional DOTmLPF-P analysis may be completed as required to fully define the DCR.

2.2.2.2. A Joint DCR may be generated without an associated ICD if non-materiel approaches appear to be the most viable solution for identified capability requirements. The Sponsor will provide ICD content, including capability requirements and capability gap table, in the appropriate successor document as outlined in the Joint DCR document formats. A Joint Staff Gatekeeper approved ICD waiver is not required for Joint DCRs without associated ICDs.

2.2.2.3. ICDs that require significant DOTmLPF-P changes, as enablers to a recommended materiel approach may be staffed in parallel with the complementary Joint DCR.

2.2.3. Combining and splitting sequences of capability requirements document.

2.2.3.1. One ICD may lead to the creation of multiple CDDs and/or DCRs, each of which contribute to satisfying the capability requirements and eliminating or mitigating identified capability gaps in the ICD.

2.2.3.2. Two or more ICDs may lead to the creation of a single CDD, where the capability solution to be developed satisfies more than one capability requirement and eliminates or mitigates more than one associated capability gap.

2.2.4. Related increments of capability requirements documents.

2.2.4.1. An ICD may lead to the creation of multiple CDDs to describe a System of Systems (SoS) approach or a single CDD with multiple annexes to describe a FoS approach or for incremental development.

2.2.4.1.1. For an SoS, where a set of systems are integrated to deliver a unique capability solution, the Sponsors should develop individual CDDs for each system within the SoS.

2.2.4.1.2. In an FoS, where similar capabilities are provided through different approaches to achieve similar or complementary effects, the Sponsor may choose to use CDD annexes to specify individual performance attributes for each individual system in the FoS. In this case, they can validate the base CDD and all CDD annexes at the same time.

2.2.4.1.3. Sponsors may choose to develop capability in increments over time through the use of CDD annexes. In this case, they may validate a base CDD for the first increment, and then use annexes, separated by time, to validate subsequent increments of the capability. More detailed information on Incremental CDD development is provided in Annex A to Appendix C of Enclosure B of this manual.

2.3. Required DoDAF Views. DoDAF views submitted will be determined by the Sponsor where no joint integration aspects are present. Views applicable to supporting all capability requirements documents are shown in Figure A-4. These views are used to facilitate validation decision making and capability requirements portfolio management. Additional DoDAF views applicable to the net-ready certification are outlined in Figure B-20 and in Annex A to Appendix G of Enclosure B to this manual. More detail on each DoDAF view is available in Appendix H to Enclosure B of this manual and in Reference [6].

2.3.1. DoDAF views and associated data supporting the capability requirements document shall be made accessible by Sponsors through a URL to the architecture data repository. Sponsors should refer to the Warfighter Mission Area – Architecture Federation and Integration Portal (WMA-AFIP accessible through the URL in Reference [7]) for additional information. Only the DoDAF views specified by the document formats, or additional views deemed appropriate by the Sponsor, should be included in the actual capability requirements document.

2.3.2. DoDAF views and associated data submitted in support of narrowly scoped ICDs, and CDDs supporting development of materiel capability solutions, are expected to align the new or updated DoDAF views with generated enterprise architecture, with updates to the enterprise architectures made as necessary.

2.3.3. DoDAF views and associated data submitted in support of broadly scoped ICDs are expected to represent the initial or updated EA associated with the scope of the ICD.

2.3.4. Data for DoDAF views are captured to the greatest extent possible during CBAs to reduce workload when generating capability requirements documents and performing follow-on efforts. As Sponsors define new or updated capability requirements, and develop associated materiel and non-materiel capability solutions, they update submitted architecture data and associated artifacts/views rather than re-creating the architecture. In addition to saving time and effort, re-use of architecture data and associated artifacts/views reduces the likelihood of unexpected disconnects between

current and previous architectures.

Document	AV-1[1]	OV-1	OV-2	OV-4	OV-5a[2]	CV-2	CV-3	CV-6	SV-1	SV-2	SV-7	SV-8
ICD/DCR	S[3]	S[3]	S[3]	S[3]	S[3]	S[3]	S[3]	S[3]	N/A[3]	N/A[3]	N/A[3]	N/A[3]
IS-ICD[4]	S[3]	S[3]	S[3]	S[3]	S[3]	S[3]	S[3]	S[3]	N/A[3]	N/A[3]	N/A[3]	N/A[3]
CDD	S[3]	S[3]	S[3]	S[3]	S[3]	S[3]	S[3]	S[3]	S/P[3]	S/P[3]	P[3]	P[3]
IS-CDD[4]	S[3]	S[3]	S[3]	S[3]	S[3]	S[3]	S[3]	S[3]	S/P[3]	S/P[3]	P[3]	P[3]

Notes:

[1] Recommend sponsors use AV-1 to describe their architecture IAW Appendix H to Enclosure B. Reference Figure B-20 for additional artifacts/views.

[2] The OV-5a must use UJTs (and Service task list extensions, if applicable) for alignment of activities. In cases where the program supports an activity not represented in the UJTL, the shortcomings are to be identified in the activity taxonomy and considered for incorporation upon the next update of the UJTL, IAW Reference [8], and using the tools available at the URL in Reference [8].

[3] S: The Sponsor, or operational user/representative, is responsible for development of the architecture data.
S/P: The Sponsor, or operational user/representative, works jointly with the program office (depending upon program stage), to develop the architecture data. DoD Components may have additional architectural/regulatory requirements for CDDs.
N/A: Not Applicable.

[4] IS-ICDs or IS-CDDs are required to provide the DoDAF views associated with the baseline ICDs or CDDs, respectively.

Figure A- 4: DoDAF Views Supporting Capability Requirements Documents

2.4. Joint DCR.

2.4.1. The Joint DCR is the mechanism to identify and validate non-materiel approaches to closing capability gaps and meeting joint military capability requirements. This can be done either independently or in conjunction with a materiel capability solution.

2.4.2. Format: The format of the Joint DCR is included in Appendix E to Enclosure B of this manual. The content of the DOTmLPF-P solutions is included in Annex F to Appendix G of Enclosure B to this manual.

2.4.3. Implementation: The Sponsor of a Joint DCR or designated lead organization and/or assigned OPRs is/are responsible to complete the tasks identified in the validated Joint DCR within the timeline delineated in the validation JROC Memorandum (JROCM). These tasks shall be supported by the chair of the Lead FCB and the affected Joint DOTmLPF-P Functional Process Owners (FPOs) identified in Figure B-25 of Annex F to Appendix G of Enclosure B in this manual.

2.4.3.1. The FCB Chair must maintain awareness of the implementation progress.

2.4.3.1.1. In cases where a Sponsor or designated lead organization proposes an altered timeline or approach to implementing the Joint DCR, the Sponsor must assess the operational risk as well as the impact the change has upon enabling or enabled capability solutions. The changes will be proposed via the Joint Staff Gatekeeper and the Lead FCB chair. Approved changes will be

documented and attached to the authoritative copy of the validated Joint DCR in the KM/DS system.

2.4.3.1.2. The FCBs are responsible for coordinating assigned tasks with the Sponsor or designated lead organization via FCB processes, and for providing periodic updates on implementation progress to the FCB O-6 and FCB General Officer/Flag Officer (GO/FO) Integration Groups.

2.4.4. Documenting completion. When the Lead FCB determines that all tasks associated with a Joint DCR are complete, the FCB Chair shall document completion in a memorandum to be posted with the original Joint DCR and validation memorandum in the KM/DS system.

2.5. Information Systems (IS) Development.

2.5.1. Sponsors should consider the IS-ICD or IS-CDD variant for capability requirements likely to be addressed by IS solutions, software development, and off-the-shelf hardware. Detailed format information is provided in Appendix B to Enclosure B or Appendix D to Enclosure B, respectively.

2.5.2. The IS-ICD or IS-CDD is meant to streamline applicable requirements processes and provide Sponsors the flexibility to manage IS capability requirements with alternate documents and validation processes as long as development efforts remain within the boundaries of the validated Information Technology (IT)-Box. However, the Sponsor must still ensure that they are compliant with acquisition policy and processes in References [5] and [9], and the Information Support Plan (ISP) policy and processes IAW Reference [10].

2.5.3. Joint command and control (C2) requirements that have a validated IS-ICD or IS-CDD will be identified, documented, validated, prioritized, managed, and monitored IAW [11].

2.5.4. The following example of documents used for managing follow-on efforts is intended to be illustrative and is not intended to limit potential flexibilities provided by the IS-ICD or IS-CDD. For the purpose of this example, two document types have been created and illustrated in Figure A-5, the Requirements Definition Package (RDP) and the Capability Drop (CD). Actual names, content, and approval process are at the discretion of the delegated oversight authority.

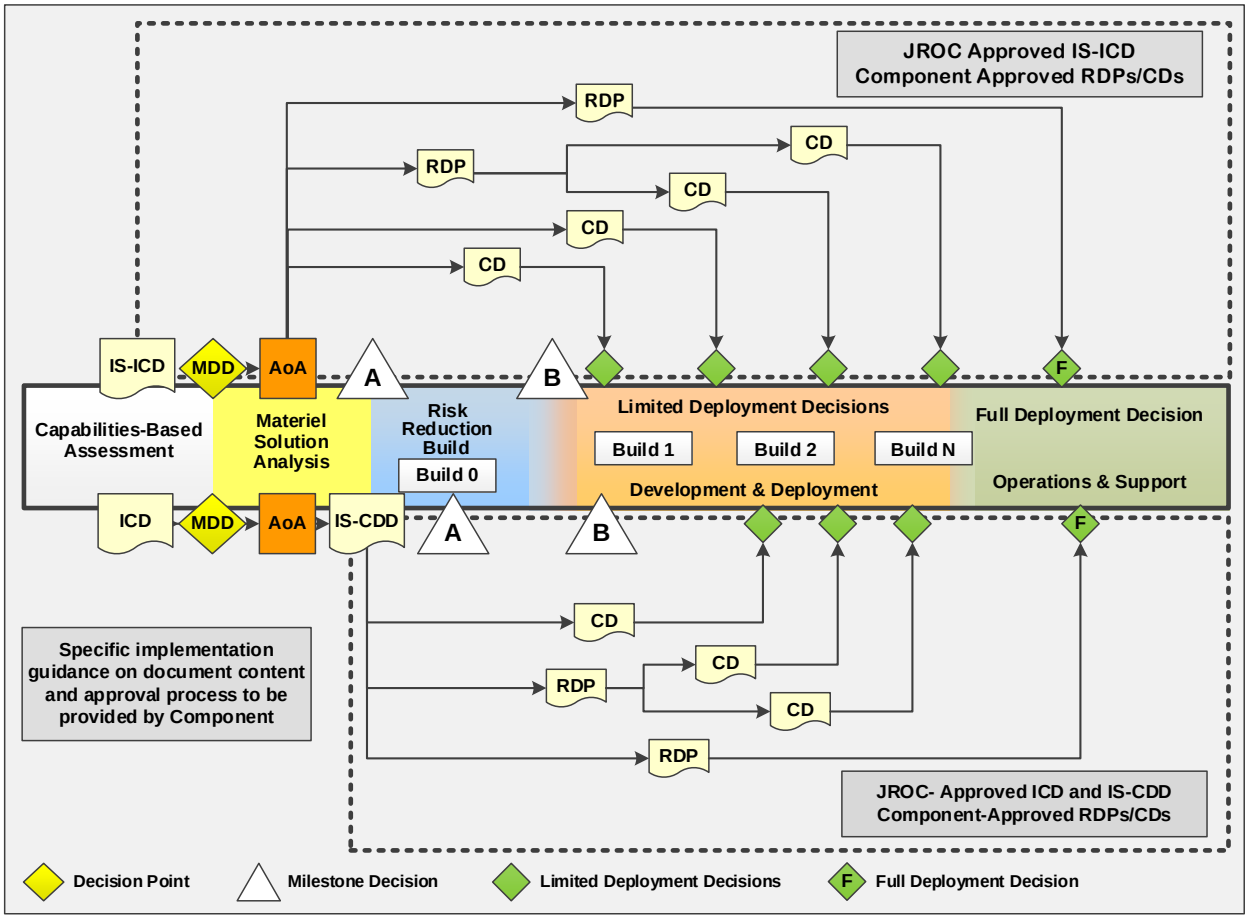

Figure A- 5: Example of IS-ICD and IS-CDD Successor Documents

2.5.4.1. A key difference in usage of IS-ICDs and IS-CDDs is whether the AoA (or like study) takes place before or after delegating authorities under the IT box.

2.5.4.1.1. For an IS-ICD to be appropriate, it must be very clear from the CBA that an IS solution is the only viable approach to be considered. The AoA (or like study) conducted in the MSA phase takes place after delegating authorities under the IT box and will therefore only consider IS solutions.

2.5.4.1.2. An IS-CDD is more appropriate when an IS solution is not presumed at the time the ICD is validated and the MDD approved, or other materiel and/or non-materiel solution(s) are expected to be necessary along with the IS solution. The IS-CDD is a result of the AoA (or like study) conducted in the MSA phase and represents an IS solution for part or all of the capability requirements validated in the ICD.

2.5.4.2. Regardless of successor documents used, the Sponsor must satisfy the net-ready certification and any acquisition activities dependent upon content from capability requirements documents.

2.5.5. The RDP (or equivalent) is a first level refinement of one or more capability requirements identified in an IS-ICD or IS-CDD and is co-developed by the operational user (or representative) and the program office. The RDP (or equivalent) identifies the KPPs, KSAs, and APAs necessary to scope and cost the implementation of a capability solution. The RDP (or equivalent) may also identify non-materiel changes that need to be implemented to fully realize the IS capability solution. The RDP (or equivalent) is approved by the delegated oversight authority identified in the IS-ICD or IS-CDD.

2.5.5.1. In the case of an IS-ICD, one or more RDPs (or equivalents) could be the equivalent of a CDD in terms of providing greater specificity of a capability solution intended to address part or all of the capability requirements identified in the IS-ICD.

2.5.5.2. In the case of an IS-CDD, a RDP (or equivalent) may not be necessary if the required level of specificity for the capability solution is already contained in the IS-CDD. However, RDPs (or equivalents) may still be used if needed to decompose the overall capability requirements of the IS-CDD into more manageable parts to facilitate the development efforts.

2.5.5.3. One or more RDPs (or equivalents) together could represent the total set of capability solutions developed to satisfy the capability requirements in the IS-ICD or IS-CDD.

2.5.5.4. In support of Reference [5], a draft RDP (or equivalent) shall be used before validation to support Milestone A decisions for IS technology/prototyping efforts. The RDP (or equivalent) shall be submitted to the delegated oversight authority for validation ahead of a Milestone B decision.

2.5.5.5. Within 14 days of validation by the delegated oversight authority, the Sponsor shall provide the RDP (or equivalent), along with its associated approval memorandum, to the Joint Staff Gatekeeper situational awareness, tracking, visibility and other information purposes. The information provided will be used to support capability requirements portfolios managed IAW Enclosure C of this manual.

2.5.5.6. The RDP (or equivalent) could then be used in multiple ways. It could be used to initiate an IS program to develop, test, and deliver the full capability solution defined in the RDP (or equivalent). It could also be used as a basis for defining multiple software builds of incremental capability solutions documented in something like a CD (or equivalent).

2.5.5.7. The Sponsor must conduct an AoA if the IS program has a projected lifecycle cost that is designated an MDAP.

2.5.6. The CD (or equivalent) describes the performance characteristics of a relatively small increment of a capability solution included in a software build necessary for partial deployment of the overall capability solution, which is typically developed and fielded within a short period of time. It could be developed through a rapid prototyping effort with the user to ensure it meets

their needs. A CD (or equivalent) could be developed directly from the definitions in the IS-ICD in the event of a more timely need for the capability solution. More commonly, multiple CDs (or equivalents) would be derived from an RDP (or equivalent) or IS-CDD to deliver the overall capability solution defined in the RDP (or equivalent) or IS-CDD.

2.5.7. If not already covered by the ISP associated with the RDP (or equivalent) or IS-CDD, the Sponsor must submit an ISP in support of the CD (or equivalent) separately to DoD CIO for certification purposes IAW Reference [12]

2.5.7.1. The approval of CDs (or equivalents) may be delegated to a lower level requirements authority as determined by the delegated oversight authority to ensure timely decision-making.

2.5.8. Deployment decisions are made by the MDA whenever the capability solution - whether developed from an RDP, a CD, or equivalents - is ready for deployment to the user.

2.5.9. Annual/Biennial FCB Review. For all IS programs with a valid IS-ICD, the Sponsor shall provide the Lead FCB an update a year following the validation and then biennially after. For an IS-CDD, the Sponsor shall provide the Lead FCB an update every second year following the validation. The Lead FCB will determine if the JROC or JCB should review the following items and will make appropriate recommendations for action.

2.5.9.1. Progress in delivering capability solutions within the required timeframe and available funding.

2.5.9.2. Compliance with applicable EA and IS data standards.

2.5.9.3. Other items as identified by the IS-ICD or IS-CDD validation.

2.6. JCIDS Interaction with Acquisition. Deliberate acquisition begins when an appropriate MDA considers a validated ICD identifying one or more capability requirements that may be best addressed with a new materiel capability solution. The MDD is documented in an Acquisition Decision Memorandum (ADM) IAW References [5] and [9]. The ADM may also direct entry at the appropriate acquisition phase, depending upon the maturity of potential capability solutions for the validated capability requirements.

2.6.1. Interaction of JCIDS Deliberate Path and the Defense Acquisition System (DAS). Each of the planned reviews below are key aspects of ensuring that appropriate tradeoffs are made among lifecycle cost, schedule, performance, and procurement quantities in the establishment and approval of joint military capabilities IAW Reference [2]. See Figure A-6 for the nominal process overview and see Enclosure B of this manual for additional detail related to documents and sequence variations.

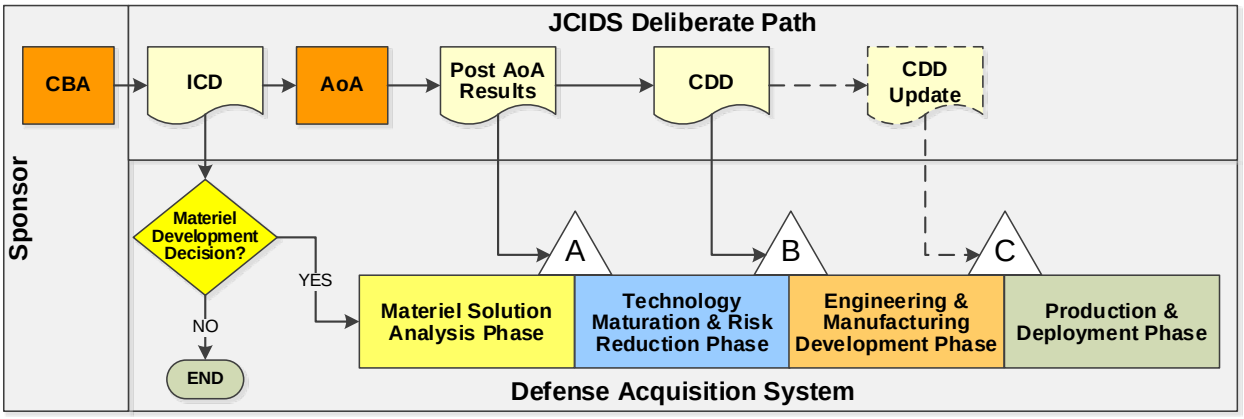

Figure A- 6: Interaction of JCIDS Deliberate Path and Defense Acquisition Systems

2.6.1.1. ICD Validation.

2.6.1.1.1. Prior to validation, the draft ICD provides the validation authority and the primary stakeholders the opportunity to assess the joint military capability, identify the associated capability gaps, and determine the impact on their capability requirements portfolios. During staffing, the validation authority and the primary stakeholders have the opportunity to recommend modifications to the document to best address the needs of the joint force and to manage and prioritize their capability requirements portfolios.

2.6.1.1.2. The validated ICD is a critical entry criterion for the MDD and guides the Sponsor's activities during the MSA phase of acquisition. This includes criterion assessed by potential materiel solutions identified in an AoA or similar study, any associated DOTmLPF-P changes, and development of other required acquisition information for the Milestone A review.

2.6.1.2. Post-AoA (or similar study) Review.

2.6.1.2.1. Following the completion of the AoA, or similar study, the Sponsor will provide primary stakeholders the opportunity to assess how the different alternatives address the validated joint military capability and associated capability gaps, to ensure the critical dependencies/enablers and assumptions have been considered, and to understand the associated lifecycle costs. It also provides the opportunity to review the results of other activities completed during the MSA phase of acquisition, and the proposed KPPs, KSAs, and APAs for the recommended alternative(s).

2.6.1.2.2. For Major Defense Acquisition Programs (MDAPs), upon completion of the Post-AoA review, the validation authority will provide a JROCM or Component level memorandum that endorses the AoA results and provides recommendations to the MDA, pursuant to Title 10 U.S.C. § 2448a (Reference [13]), for program costs and fielding targets.

2.6.1.2.2.1. These program costs and fielding target recommendations are approved through a separate process, known as the Investment Review Process

recently established per Section 925(b) of the FY17 NDAA as depicted in Reference [14].

2.6.1.2.2.2. The JROC, JCB, or independent validation authority as described in Appendix C of Enclosure A of this manual will provide recommendations to the Investment Review Process that will require a level of resources consistent with the priority assigned to the capability gap and have an estimated time of delivery of an Initial Operational Capability (IOC) that is consistent with the urgency of the associated capability gap to evolve system capabilities and improve interoperability.

2.6.1.2.2.3. Program costs and fielding targets (as mandated under Reference [13]) will be approved by the SecDef, or delegated to the DepSecDef, before funds can be obligated for technology development, systems development, or production. These program costs and fielding targets are defined in Title 10 U.S.C. § 2448a as goals for procurement unit and sustainment cost, IOC date, technology maturation, prototyping and the use of a modular open system approach.

2.6.1.2.3. The Post-AoA review shall allow for sufficient time prior to completion to permit Sponsor preparation and approval of the draft CDD to inform both the development of the RFPs in support of the Technology Maturation and Risk Reduction (TMRR) phase of acquisition and the Milestone A decision. The CDD that is prepared and approved by the Sponsor is a critical criterion for the Milestone A decision. The draft CDD is not provided to the Joint Staff Gatekeeper for staffing and validation submission at that time.

2.6.1.2.4. In cases where Milestone A is not required, the review by the validation authority shall be completed before the next directed Milestone or the release of the RFP for the subsequent phase of acquisition, whichever comes first. If a formal AoA or similar study is not appropriate, the MDA will coordinate with the validation authority to ensure that the validation authority has the proper information to advise the MDA.

2.6.1.3. CDD validation.

2.6.1.3.1. Review of the CDD provides the validation authority and the primary stakeholders the opportunity to assess how the proposed capability solution, its associated performance attributes, and other supporting data, fulfill the gap/gaps in the validated ICD.

2.6.1.3.2. During staffing, the validation authority and the primary stakeholders have the opportunity to recommend modifications to the document to best address the needs of the joint force and to manage and prioritize the capability requirements portfolios.

2.6.1.3.2.1. The performance attributes set in the CDD do not necessarily need to achieve 100 percent of the initial objective values validated in the ICD. The validation authority and the primary stakeholders will assess the operational

risk and impact on the capability requirements portfolios of performance above or below the validated values.

2.6.1.3.2.2. Establishing performance attributes that reflect the best path to obtaining an optimal return on investment with respect to the initial objective values validated in the ICD is a key aspect of incorporating knowledge gained during the MSA and TMRR phases of acquisition. This ensures that appropriate tradeoffs are being made among lifecycle cost, schedule, performance, and procurement quantities to manage and prioritize the capability requirements portfolios.

2.6.1.3.2.3. Active engagement between the program office and the requirements sponsor during development and review of proposed requirements trades is essential to ensure requirements trades are fully informed by systems engineering trade-off analyses and are technically achievable, affordable, and testable.

2.6.1.3.3. When the JROC is the validation authority, evidence of determination by the Service Chief must be provided prior to submitting the document to the JROC for validation. The Sponsor will ensure that the written determination provided by Service Chief indicates that the requirements are necessary and realistic in relation to program cost and fielding targets established under Title 10 U.S.C. § 2448(a) and Title 10 U.S.C. § 2547 (References [13] and [15]). This written determination can either be provided by the Service Gatekeeper prior to validation or can be considered accomplished via the JROCM or like Memorandum validating the CDD.

2.6.1.3.4. The validated CDD is a requirement for the Development RFP release decision point and informs the Milestone B decision. The validated CDD is a key factor in the MDA decision to initiate an acquisition program at Milestone B and guides the Sponsor's activities during the EMD phase of acquisition. In cases where the MDA waives Milestone B but an EMD phase of acquisition will be conducted, the CDD shall be validated before RFP release for the EMD phase of acquisition or the beginning of the EMD phase of acquisition, whichever comes first.

2.6.1.3.5. In the case where the MDA allows a program to enter at Milestone B or C, a validated CDD will be required prior to the Milestone B or C decision.

2.6.1.4. CDD Updates.

2.6.1.4.1. The Sponsor may update the CDD based on knowledge gained during source selection and EMD phase activity. It is likely performance attributes set in the initial CDD will change as more information is gained. In these cases, the Sponsor shall submit the updated CDD for review and revalidation by the approval authority IAW the deliberate staffing section of this appendix.

2.6.1.4.2. A CDD Update will follow the deliberate staffing process outlined in this appendix. During these updates, primary stakeholders will have the

ability to review and provide comment only on the updated parts of the document as approved by the Joint Staff Gatekeeper (when JCB or JROC is the validation authority) and in consultation with the document Sponsor. For non-JCB or JROC Interest documents or other non-joint issues, the Sponsor may accept or decline any additional commenting at the discretion of the independent validation authority or otherwise, as appropriate. Primary stakeholders may request, with valid reasons, that the Joint Staff Gatekeeper allow review and comment on other sections of the document.

2.6.1.4.3. In cases where there are only minor changes to the CDD, but the Sponsor still chooses to have the document revalidated by the JROC, the Sponsor may submit a written request to the Joint Staff Gatekeeper for review and expedited staffing. At a minimum, minor changes will be reviewed by the FCB Chair, the Deputy Director for Requirements and Capability Development (DDRCD), and JCB.

2.6.1.4.4. In cases where there are no changes to a CDD, Sponsors may proceed directly to the subsequent milestone decision without revalidation. The validated CDD and validation memo will provide the necessary requirements documentation IAW Reference [5].

2.6.2. Interaction of JCIDS Incremental Path and the DAS. The Incremental Path as depicted in Figure A-7 provides the Sponsor flexibility to define capabilities from a base CDD to address both an incremental development approach and FoS approach.

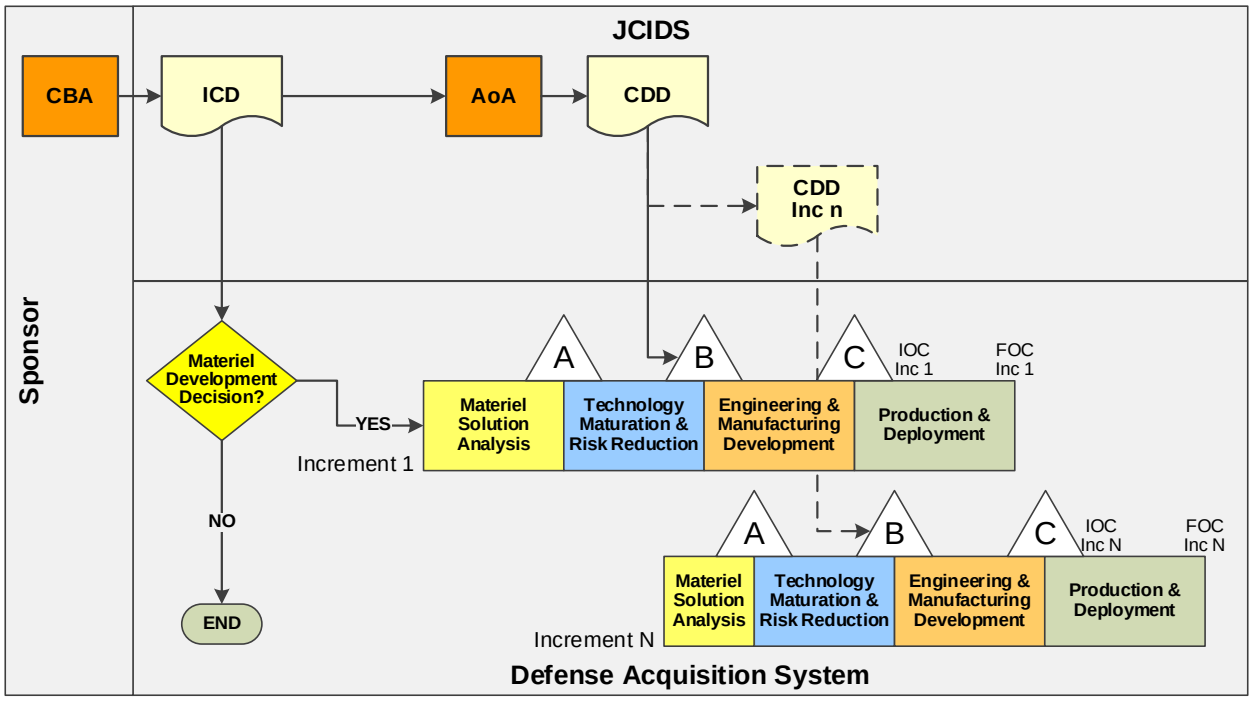

Figure A- 7: Interaction of JCIDS Incremental Path and Defense Acquisition System

2.6.2.1. Incremental Development. In an incremental development approach for capabilities, a Sponsor describes the system and performance attributes of the initial capability solution in a base CDD. As incremental capability is added to the base system over time, or block upgrades are developed, the Sponsor may document this in an annex to the base CDD.

2.6.2.2. In an FoS approach with a single Sponsor, the Sponsor may develop a base CDD and concurrently staff annexes for individual systems within the family. The base CDD will specify attributes for the entire FoS and each annex will specify additional attributes for the individual systems.

2.6.3. Interaction of JCIDS Information Systems Path and DAS. The information systems path as depicted in Figure A-8 provides the Sponsor flexibility where deployment of the full capability of a software intensive program will occur in multiple increments as new capability is developed and delivered. The period of each increment should not be arbitrarily limited. The length of each increment and the number of deployable increments should be tailored and based on the logical progression of development and deployment for use in the field for the product being acquired.

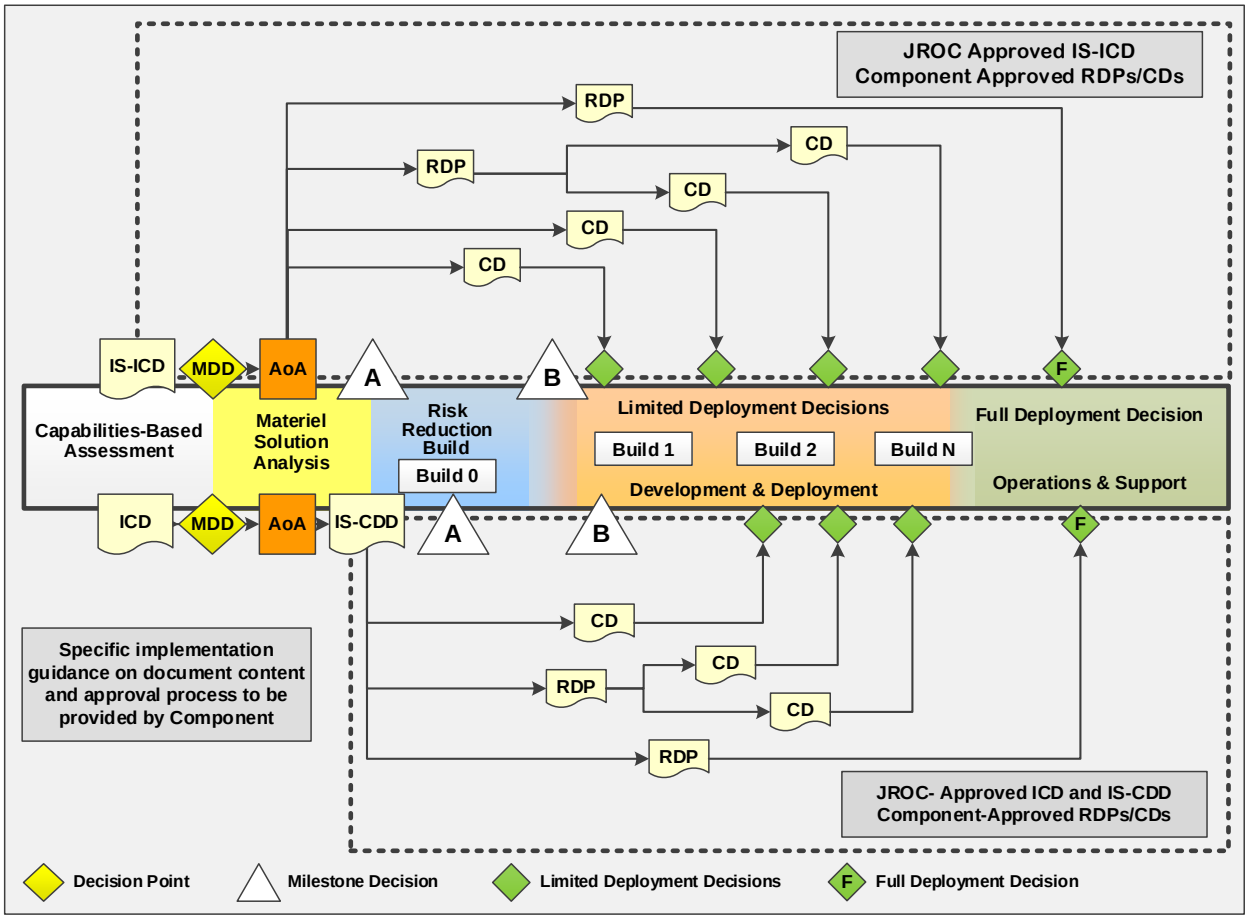

Figure A- 8: Example of IS-ICD and IS-CDD Successor Documents

3. JCIDS Deliberate Staffing.

3.1. General Staffing Guidelines.

3.1.1. Primary Stakeholders in Document Review.

3.1.1.1. Primary Stakeholders are those organizations with a direct interest and a clear equity in the capability document submitted for staffing.

3.1.1.2. Capability requirements documents contain content that is of interest to, or may have impact upon, many different stakeholders across the joint force in addition to the Services and CCMDs, including but not limited to those shown in Figure A-9.

Capability Requirements Documents			Section Primary Equities	
ICD (or IS-ICD)	**Joint DCR**	**CDD (or IS-CDD)**	**Joint Staff**	**Other/Advisors**
Operational Context	Operational Context	Operational Context	J-3 and J-5	CAPE (for ISCs)
Threat Summary	Threat Summary	Threat Summary	J-283/IRCO	USD(I)
Capability Requirements/ Capability Gaps	Capability Discussion	Capability Discussion	FCBs, J-4/ED, J-4/MMSD, J-8/CAD, J-8/JCD, and J-8/PBAD	USD(I), USD(R&E), USD(A&S), DoD CIO, and DOT&E
N/A for ICDs (or IS-ICDs)	N/A for Joint DCRs	Program Summary		
N/A for ICDs (or IS-ICDs)	N/A for Joint DCRs	Performance Attributes KPPs/KSAs/APAs		
N/A for ICDs (or IS-ICDs)	N/A for Joint DCRs	Other System Attributes	FCBs and J-8/JCD	USD(R&E), USD(A&S), and DOT&E
N/A for ICDs (or IS-ICDs)	N/A for Joint DCRs	Interoperability	J-6/C4Cyber and J-7	USD(A&S), USD(R&E), and DoD CIO, and DOT&E
N/A for ICDs (or IS-ICDs)	N/A for Joint DCRs	Spectrum Requirements	J-6/C4Cyber	USD(R&E), USD(A&S), and DoD CIO, and DOT&E
N/A for ICDs (or IS-ICDs)	Intelligence Supportability	Intelligence Supportability	J-283/IRCO	USD(I)
N/A for ICDs (or IS-ICDs)	N/A for Joint DCRs	Weapon Safety Assurance	J-8/FPD	JWSTAP and USD(A&S)
N/A for ICDs (or IS-ICDs)	N/A for Joint DCRs	Technology/ Manufacturing Readiness	FCBs, J-8/JCD, J-8/CAD, and J-8/PBAD	USD(R&E)
N/A for ICDs (or IS-ICDs)	Change Recommendations	DOTmLPF-P Considerations	J-1, J-4, J-5, J-7, and J-8/FD	USD(P), USD(P&R), and USD(A&S)
Recommendations	Resource Summary	Program Affordability	Validation Authority	MDA and CAPE

Figure A- 9: Primary Equities in JCIDS Documents

3.1.1.3. It is critical that primary stakeholders review and comment upon capability requirements documents to ensure that proposed new capability

requirements or changes to validated capability requirements are aligned with the needs of the joint force and are consistent with the NMS. As capability requirements documents are intended to address operational needs, comments from stakeholders should be only those required to ensure alignment with the overall needs, priorities, and policies of the joint force, and not unduly replicate content which exists, or should exist, in other documents or policies.

3.1.1.4. The review by primary stakeholders is not to be a cursory evaluation of content and formatting; rather it is designed to provide both:

3.1.1.4.1. A robust understanding of implications to the warfighter and the capability requirements portfolios, and;

3.1.1.4.2. A robust understanding of how validation of the capability requirements may impact stakeholder processes and other equities. Any approved waivers will be published to ensure visibility.

3.1.1.5. Joint Staff certifying and endorsing organizations.

3.1.1.5.1. Each of the organizations responsible for certifications and endorsements, as identified in Figure A-16 of Appendix C to this enclosure, reviews documents and provides comments if changes to the document are required prior to providing the certification or endorsement. All Joint Staff certifications and endorsements, and/or any associated waivers, will be submitted via memorandum format IAW Appendix C of this manual.

3.1.1.5.2. In cases where a certification or endorsement is not applicable to a document, these organizations will provide a hard copy memorandum or KM/DS note in lieu of certification or endorsement stating it is not required.

3.1.1.5.3. Comments from the certifying or endorsing organization are authoritative with respect to their certification or endorsement. Other stakeholders submit comments related to the certification or endorsement via the certifying or endorsing organization for potential inclusion in the authoritative direction.

3.1.1.6. Sponsor certification and endorsement.

3.1.1.6.1. Sponsor organizations will have authority to certify or endorse all performance attributes that are not designated JPRs regardless of JSD assignment. This includes the threat assessment/intelligence certification and DOTmLPF-P endorsement for capability requirements documents assigned a JSD of Joint Information. See Figure A-16 in Appendix C to this enclosure for specific certification and endorsement responsibilities.

3.1.1.6.2. Sponsors should engage early with Joint Staff certifying and endorsing organizations when developing their capability requirements document. This includes those documents in which they have independent validation authority or performance attributes that are not designated JPRs to leverage off the processes used by the joint certification organizations. This will help Sponsors gain the benefit of Joint Staff insight without be held to the

deliberate staffing timeline and increase the likelihood of a creating a better product for formal staffing.

3.1.1.6.3. Sponsors will be responsible for providing evidence of their applicable certifications or endorsements (which may be incorporated into the Sponsor validation memo) along with the capability requirements document to the Joint Staff Gatekeeper.

3.1.2. Comment Submission. All comments are due by the end of the initial staffing period.

3.1.2.1. Types of comments.

3.1.2.1.1. Administrative. Recommendations to fix formatting, grammatical, or typographical errors, or to change writing style to make the document easier to read and understand. Comments do not substantively change the content of the document.

3.1.2.1.2. Substantive. Recommendations to make minor or moderate changes to better align the document with the needs of the joint force or applicable policy/guidance, or to correct or clarify minor factual inaccuracies. Considered to be a "Concur, with comment" response to the staffing, but scope and quantity of several substantive comments may also lead to a "Non-concur" response to the staffing until satisfactorily adjudicated.

3.1.2.1.3. Critical. Recommendations to make significant or comprehensive changes to better align the document with the needs of the joint force or applicable policy/guidance, or to correct significant factual inaccuracies that are in conflict with authoritative guidance. Critical comments also may address text or issues which would otherwise be considered substantive, but if not corrected would prevent the document from serving its intended purpose, lead to the withholding of a mandatory certification or endorsement, or result in disapproval by the validation authority. Considered a "non-concur" response to the staffing until satisfactorily adjudicated.

3.1.2.2. Comment coordination.

3.1.2.2.1. Critical comments are to be approved for submission at the GO/FO or SES level. Substantive comments are expected to be approved for submission at the O-6 or GS-15 level. Administrative comments may be approved for submission below the O-6 or GS-15 level. Commenters may be required to justify the level of comment at the appropriate level of oversight body: FCB, O-6 Integration, GO/FO Integration, JCB, or JROC.

3.1.2.2.2. Submitted comments are to indicate both the name/rank of the approver and the name/rank and contact information for the AO with which the Sponsor can work to adjudicate the comments. In cases where a negotiated adjudication is different from the intent of the initial comment, the AO will ensure that the comment approver concurs with the adjudication or that the open issue continues to be discussed at follow-on steps of the process until adequately adjudicated.

3.1.2.2.3. Organizations/agencies making comments as part of staffing will coordinate comments through a single organizational Gatekeeper.

3.1.2.3. Comment Classification. Comments are submitted in a manner dependent upon their classification level and Alternative Compensatory Control Measure (ACCM) or Special Access Program (SAP)/Special Access Required (SAR) protections.

3.2. JCIDS Deliberate Staffing Process. Capability requirements documents (ICDs, IS-ICDs, Joint DCRs, CDDs, or IS-CDDs) with a Joint Staffing Designator (JSD) of JROC or JCB Interest are reviewed and validated IAW this enclosure. One exception is that Special Operations Peculiar (SO-P) documents or joint Cyberspace Operations (CO) capability requirements assigned a JSD of JCB Interest or below are reviewed and validated IAW Reference [16] and [17] respectively. See Figure A-10 and Figure A-11 below for a depiction of the staffing timelines for JROC and JCB Interest documents.

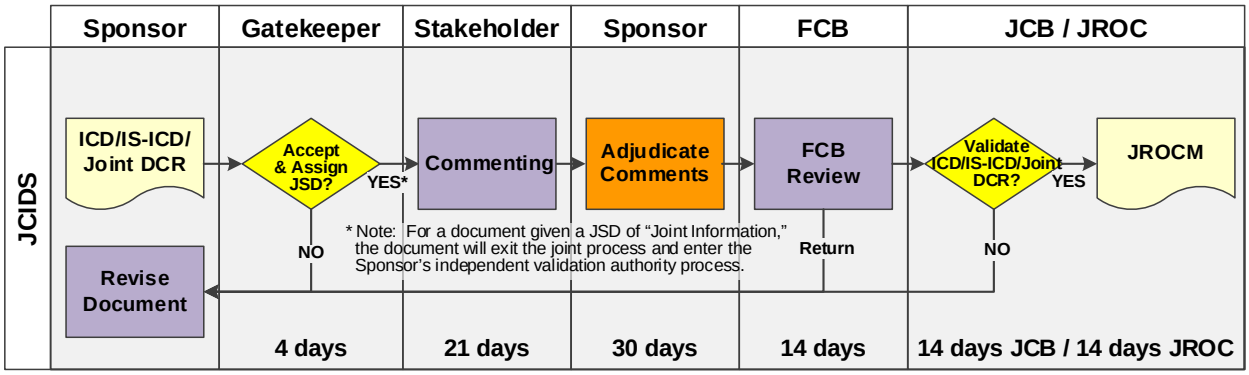

Figure A- 10: JCIDS Deliberate ICD, IS-ICD, and Joint DCR Staffing (97 days)

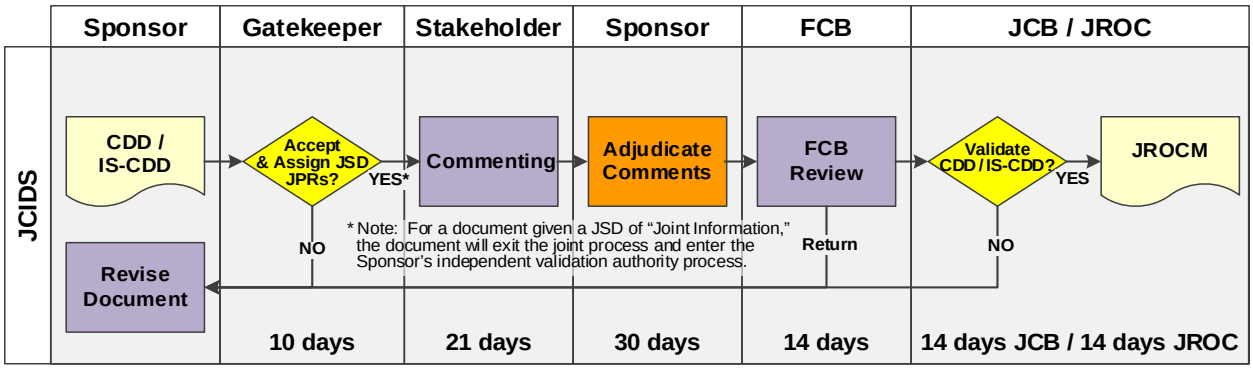

Figure A- 11: JDICS Deliberate CDD ad IS-ICD Staffing (103 days)

3.2.1. Staffing Timelines. The deliberate staffing process for a properly prepared ICD, IS-ICD, or Joint DCR takes no more than 97 days and for the CDD or IS-CDD takes no more than 103 calendar days.

3.2.1.1. The Joint Staff Gatekeeper may consider requests from Sponsors for extensions to staffing timelines. In order to ensure proper consideration, Sponsors should provide valid reasons for these requests.

3.2.1.2. A Sponsor may withdraw a document provided to the Joint Staff Gatekeeper, or from staffing at any time after submission into JCIDS, with notification to the Joint Staff Gatekeeper. If this occurs and the Sponsor wants to re-submit the document, it will enter the process at the Gatekeeper phase as a new document.

3.2.1.3. While timely review and validation of JCIDS documents is a goal, the best measure of success for the staffing process is when the FCB Chairs, certification and endorsement organizations, and other stakeholders, have a clear understanding of and can recommend to leadership how a new or modified capability requirements and supporting data within the document represents the best tradeoff in performance, cost, schedule, and quantity to minimize unnecessary redundancy and meet the needs of the joint force.

3.2.1.4. Sponsors are encouraged to engage with the primary stakeholders, as depicted in Figure A-9, of the JCIDS process at any time prior to staffing to help ensure that capability requirements documents are developed in a way that will not require significant rework during staffing. This is important in cases where the Sponsor intends to request waivers of any certifications or endorsements, or other deviations from the process.

3.2.2. Staffing Phases.

3.2.2.1. Initial Review (Joint Staff Gatekeeper and select stakeholders) (ICD, IS-ICD, or Joint DCR=4 calendar days; CDD/IS-CDD=10 calendar days).

3.2.2.1.1. Initiation. The deliberate staffing process begins when the Joint Staff Gatekeeper, after screening and review, submits the document into JCIDS. Initial review of the document(s) is conducted within 4 calendar days for an ICD, IS-ICD, or Joint DCR and 10 days for a CDD or IS-CDD.

3.2.2.1.2. Selected primary stakeholders may be asked by the Joint Staff Gatekeeper to provide an initial review of a document or issue as part of activities described in Appendix C to this enclosure.

3.2.2.1.2.1. These actions include time for the Sponsor, Lead FCB, and Joint Staff Gatekeeper to review, assign JSD and designate JPRs.

3.2.2.1.2.2. The J-8 Deputy Director for Requirements and Capability Development (DDRCD) has the authority to assign JSDs and designate JPRs. If there is a dispute between the Sponsor, Lead FCB, and Joint Staff Gatekeeper over the JSD assignment or JPR designation then further staffing will be conducted until final resolution. This staffing may require JCB or JROC adjudication of JSD assignment or JPR designation.

3.2.2.2. Document Review and Commenting (Formal staffing and commenting by stakeholders) (21 calendar days).

3.2.2.2.1. Document review and commenting is conducted with the Services, CCMDs, Joint Staff, and other DoD Agencies, as well as certifying/endorsing organizations and other primary stakeholders. For SAP/SAR or ACCM

protected documents, the J-8/SAPCOORD and Joint Staff Gatekeeper will ensure appropriately cleared AOs and FCB Chairs with equity in the document are read-in to the program and related program(s) in the capability requirements portfolio(s) as needed to review and comment.

3.2.2.2.2. Key points for primary stakeholders to understand include, but are not limited to:

3.2.2.2.2.1. What problem are we trying to solve and for whom? What CCMDs are impacted, and are they supportive of the proposed changes? What is the timing of the capability requirements and why?

3.2.2.2.2.2. How does this support the NDS and enable execution of primary DoD missions, such as identified in the Joint Strategic Capabilities Plan (JSCP)? Which JSCP missions does this requirement support?

3.2.2.2.2.3. What operational risks, and for what missions/tasks, is the joint force buying down with a proposed capability solution to identified capability requirements and associated capability gaps? For CDDs and IS-CDDs are the performance attributes traceable to the operational tasks and capability requirements they support, and do the KPPs reflect the parameters most critical to mission effectiveness?

3.2.2.2.2.4. What joint alternatives could be pursued in lieu of developing a new capability solution? What missions/tasks cannot be completed by any alternatives across the joint force while a capability solution is developed?

3.2.2.2.2.5. Where is the optimal return on investment for cost/performance tradeoffs? Who has conducted independent review or analysis, and do we understand the reasons for any differences in results?

3.2.2.2.2.6. Where is the money coming from? Unless sustained budgetary increases will fund the capability solution over its lifecycle, what other capabilities will be reduced or eliminated to provide resources for a new capability solution? What are the operational risks, or missions/tasks that cannot be performed, that result from these choices?

3.2.2.2.2.7. If the capability requirements are validated in the JCIDS process, what implications result for stakeholder processes and other equities?

3.2.2.3. Comment Adjudication Stage (30 calendar days).

3.2.2.3.1. Following initial review and commenting, the Sponsor adjudicates comments. Sponsors are to work with stakeholders to adjudicate comments to the greatest extent possible during the comment adjudication stage. At the end of the 30-day period, Sponsors shall bring forward documents that have comments which have not been adjudicated to the satisfaction of the stakeholder.

3.2.2.3.2. Comments pertaining to ICDs, IS-ICDs, and Joint DCRs with a JSD assignment of JCB or JROC Interest will be adjudicated to the satisfaction of the Lead FCB Chair (on behalf of the JCB or JROC).

3.2.2.3.3. Comments pertaining to CDDs or IS-CDDs regardless of JSD assignment, with the exception of those performance attributes (KPPs, KSAs, or APAs) designated as JPRs or areas of the document that are considered critical or essential to ensure interoperability or fulfill a gap or more than one armed force, will be adjudicated to the satisfaction of the Sponsor. Those comments that are related to JPRs or areas of the document that are considered critical or essential to ensure interoperability or fulfill a gap of more than one armed force will be adjudicated by the Lead FCB (on behalf of the JCB or JROC). Reference Figure A-16 for specific guidance on certification and endorsement authorities.

3.2.2.3.4. At any time the JROC can elevate the adjudication of a comment that pertains to a performance requirement if the Chairman of the Joint Chiefs of Staff determines it should be reviewed IAW Title 10 U.S.C. § 181(b)(5).

3.2.2.3.5. Upon completion of comment adjudication, the Sponsor submits the revised document, along with disposition of all comments and status of any unresolved comments. The revised document does not require re-staffing unless the Lead FCB Chair deems the updated document not ready for validation and recommends that the Joint Staff Gatekeeper restart the staffing process.

3.2.2.4. FCB WG and FCB Review (14 calendar days).

3.2.2.4.1. The most critical aspect of the FCB review stage is for the FCB Chair to ensure that proposed capability requirements provide best value to the warfighter without unnecessary redundancy in the capability requirements portfolio and align with the priorities of the joint force.

3.2.2.4.2. Following Sponsor comment adjudication, the FCB reviews the revised document, ensures the appropriate certifying or endorsing organizations (Reference Figure A-16) concur with Sponsor adjudication of comments, and assists the FCB Chair in reaching a recommendation for the JCB or JROC. The FCB WG and FCB are forums for identifying and discussing divergent stakeholder views. While consensus is not required to move an issue forward to the next level of review, all dissenting views will be captured and briefed to inform decision makers.

3.2.2.4.2.1. For capability requirements documents falling primarily within a single FCB, the FCB Chair makes the recommendation to the JCB or JROC. For capability requirements documents protected by ACCM or SAP/SAR designation, the FCB Chair makes the recommendation based on review and assessment by a subset of appropriately cleared AOs.

3.2.2.4.2.2. For capability requirements documents not protected by ACCM or SAP/SAR designation, with equity spread across multiple FCBs, the Lead FCB Chair will either coordinate efforts directly with the supporting FCB Chair(s) or use the FCB O-6 and FCB GO/FO Integration Groups to coordinate interdependent efforts before making the recommendation to the JCB or JROC.

3.2.2.4.2.3. For capability requirements documents protected by ACCM or SAP/SAR designation, with equity spread across multiple FCBs, the J-8/DDRCD will consolidate inputs from individual FCB Chairs and their AOs, and any other participating reviewers, and makes the recommendation to the JCB or JROC.

3.2.2.4.3. Joint Staff certifying and endorsing organizations use the same time period to review the revised document and provide a memorandum signed by an appropriate GO/FO/SES. This memorandum will either certify or endorse the document, withhold certification or endorsement of the document, or waive the need for the certification or endorsement.

3.2.2.4.3.1. When delegated to the Sponsor per Figure A-16, the Sponsor certification and/or endorsing organization(s) will provide evidence that they conducted the appropriate certification or endorsement and provide the FCB a recommendation on any outstanding issues prior to validation.

3.2.2.4.3.2. Joint Staff certification and endorsement authorities are generally expected to provide their respective certifications, or waivers thereof, prior to the meeting of the FCB. This supports the FCB Chair's recommendation to move the document on to the JCB or JROC for validation.

3.2.2.4.3.3. In cases where required data is available, there are no outstanding contentious issues, and certification or endorsement is expected prior to validation, the FCB chair may recommend that the document continue to move forward with the certification or endorsement to be provided before validation.

3.2.2.4.3.4. In cases where required data for the certification or endorsement was not provided by the Sponsor, or there are outstanding contentious issues, the FCB chair may decide to withhold recommendation to move the document forward for validation until the certification or endorsement is provided.

3.2.2.4.4. In cases where a submitted ICD or IS-ICD represents an unnecessary redundancy to approved joint military capability requirements, the FCB review may:

3.2.2.4.4.1. Recommend the Sponsor use the approved joint military capability requirements for development of a new capability solution.

3.2.2.4.4.2. Recommend that no action be taken on the capability requirements in cases where the likely costs associated with providing a capability solution outweigh the operational risk of leaving the capability gap unmitigated.

3.2.2.4.4.3. Recommend a non-materiel change to partially or wholly address the capability requirements and associated capability gaps.

3.2.2.4.4.4. Recommend other U.S. Government agency/department or allied/partner nation collaboration to partially or wholly address the capability requirements and associated capability gaps.

3.2.2.4.5. The FCB Chair is ultimately responsible for providing a positive or negative validation recommendation to the validation authority.

3.2.2.4.5.1. When submitting a positive validation recommendation to the JCB or JROC, the FCB Chair is certifying that the capability requirements, and proposed capability solutions if applicable, articulated in the document are not unnecessarily redundant to fielded capability solutions in the joint force. The FCB Chair also verifies that all required certifications and endorsements, or waivers thereof, have been obtained from the appropriate certification or endorsement authorities. Positive validation recommendations will also summarize lifecycle cost, schedule, performance, and quantity parameters, as appropriate for the document.

3.2.2.4.5.2. When submitting a negative validation recommendation to the JCB or JROC, the FCB Chair will provide the associated justification such as non-alignment with the needs of the capability requirements portfolio, lack of one or more certifications or endorsements, unresolved critical comments, etc. Unless the document is withdrawn by the Sponsor, the FCB Chair will ensure that the JCB Chair, through the Joint Staff Gatekeeper, is made aware of any ongoing efforts to reach a positive validation recommendation.

3.2.2.5. Validation (14 calendar days for JCB Interest, 28 calendar days for JROC Interest).

3.2.2.5.1. Validation Authorities.

3.2.2.5.1.1. The JROC is the validation authority for all documents that have a JSD of JROC Interest.

3.2.2.5.1.1.1. The JROC may assert itself as the validation authority for any document of any assigned JSD at any time by directing the Joint Staff Gatekeeper to set the JSD to JROC Interest.

3.2.2.5.1.1.2. The JROC may elect to validate a document through a “Paper JROC” without physically convening, when the FCB and JCB Chairs recommend validation and there are no issues for JROC discussion.

3.2.2.5.1.2. The JCB is the validation authority for all documents that have a JSD of JCB Interest.

3.2.2.5.1.2.1. The JCB may assert itself as the validation authority for any document with a JSD other than JROC Interest at any time by directing the Joint Staff Gatekeeper to set the JSD to JCB Interest.

3.2.2.5.1.2.2. The JCB may elect to validate a document through a “Paper JCB” without physically convening, when the FCB Chair recommends validation and there are no issues for JCB discussion.

3.2.2.5.1.3. The Sponsor is the validation authority for all documents given a JSD other than JROC Interest or JCB Interest.

3.2.2.5.2. The validation stage begins when the FCB Chair provides a recommendation, positive or negative. The FCB Chair briefs the validation authority with any related comments for discussion, along with the recommendation for or against validation.

3.2.2.5.3. The FCB Chair shall present any dissenting comments or issues, including any critical comments not adjudicated or certifications or endorsements not obtained. An appropriate level GO/FO or SES representative from the dissenting organization must be present at the JCB and JROC to engage in the discussion if the organization wants their comment to continue to be considered.

3.2.2.5.4. In cases where there are no issues for discussion, and the recommendation is for validation, the FCB chair may recommend a "paper" JCB and/or JROC in lieu of a physical meeting of the validation authority.

3.2.2.5.5. In support of Reference [2], the JROC, JCB, or independent validation authorities, provide review and validation that:

3.2.2.5.5.1. The proposed capability fulfills a gap in joint military capabilities.

3.2.2.5.5.2. The program cost target requires a level of resources consistent with the level of priority assigned to the associated capability gap.

3.2.2.5.5.3. The fielding target has an estimated time for the delivery of an initial operational capability that is consistent with the urgency of the associated capability gap.

3.2.2.5.5.4. The capability solutions have had appropriate consideration of tradeoffs between lifecycle cost, schedule, performance, and production quantities.

3.2.2.5.6. IAW Reference [18], validation includes agreement that the identified Service(s) will support implementation action and/or funding in related processes. In cases where changes to operations, threats, priorities, or fiscal environment may impact prior agreement to support implementation and/or funding, the Sponsor shall return to the JROC, JCB, and/or independent validation authority) for review and potential adjustment of capability requirements before POM decisions are finalized.

3.3. Post-Validation Documentation.

3.3.1. Validation decisions by the JROC or JCB are documented via JROCM and are signed by the JROC Chairman or designee. Validation decisions by Sponsors are documented by memorandum or other suitable format approved by the validation authority. Within 14 days of validation, final versions of all validated requirement documents, including their validation memorandums, are provided to the Joint Staff Gatekeeper for information purposes and visibility in the capability requirements portfolios.

3.3.1.1. The final version of the validated document will incorporate changes to the capability requirements and/or supporting information as directed or

agreed to during staffing. Note that any briefings used during the staffing process are not authoritative artifacts for the validated capability requirements, so updates to briefing materials do not satisfy the intent of this section.

3.3.1.2. In cases where validation of new or modified capability requirements in one document impose changes to other validated capability requirements, the JROCM may document required changes for the other system(s) which have been agreed upon during staffing. This negates the need for separate rounds of staffing and separate JROCMs for each affected system.

3.3.1.3. For Joint DCRs, the validation memorandum also will formalize the assignment of an OPR as agreed to during staffing. The Joint Staff Gatekeeper is authorized to approve OPR reassignment, assuming both the old and new OPR agree. The Joint Staff Gatekeeper is also authorized to approve administrative task modification and/or task deletion resulting from 'facts of life' changes such as organizational changes.

3.3.1.4. The validation decision memorandum will be inserted behind the cover page of the capability requirements document itself, replacing the validation page placeholder. A capability requirements document without the associated validation memorandum attached shall be considered draft and not yet usable for follow-on activities.

3.3.1.5. For recordkeeping, updated documents and associated validation memoranda classified at or below the level of SECRET are uploaded to the KM/DS system. Documents and associated validation memoranda classified at a level higher than SECRET are provided to the Joint Staff Gatekeeper via JWICS or via the J-8/SAPCOORD, depending upon classification.

3.3.2. Any changes made which relate directly to the substance of the document or certifications/endorsements – including KPPs, lifecycle cost, schedule, and/or quantity – render the document invalid for the purpose of any follow-on processes until revalidated by the validation authority.

3.3.3. The validation authority may rescind a previous validation and/or direct changes to or re-staffing of a validated document at any time. The validation authority will notify the document Sponsor in writing, with rationale for the rescission.

3.4. Staffing of JROC/JCB Tripwire, Classified Information Compromise Assessment (CICA) and CIP Breach Reviews. See Enclosure C of this manual for additional considerations related to Tripwire reviews.

3.4.1. The process for the JROC/JCB Tripwire review, CICA, and CIP Breach Review is illustrated in Figure A-12. The JROC/JCB Tripwire review is initiated when one or more cost, schedule, or quantity parameters set in the validation JROCM are exceeded. Note that CICA and CIP Breach reviews follow this same general process when assessing a classified information compromise or evaluating impacts of CIP changes, but are initiated under different conditions, by different organizations, with different outputs explained below.

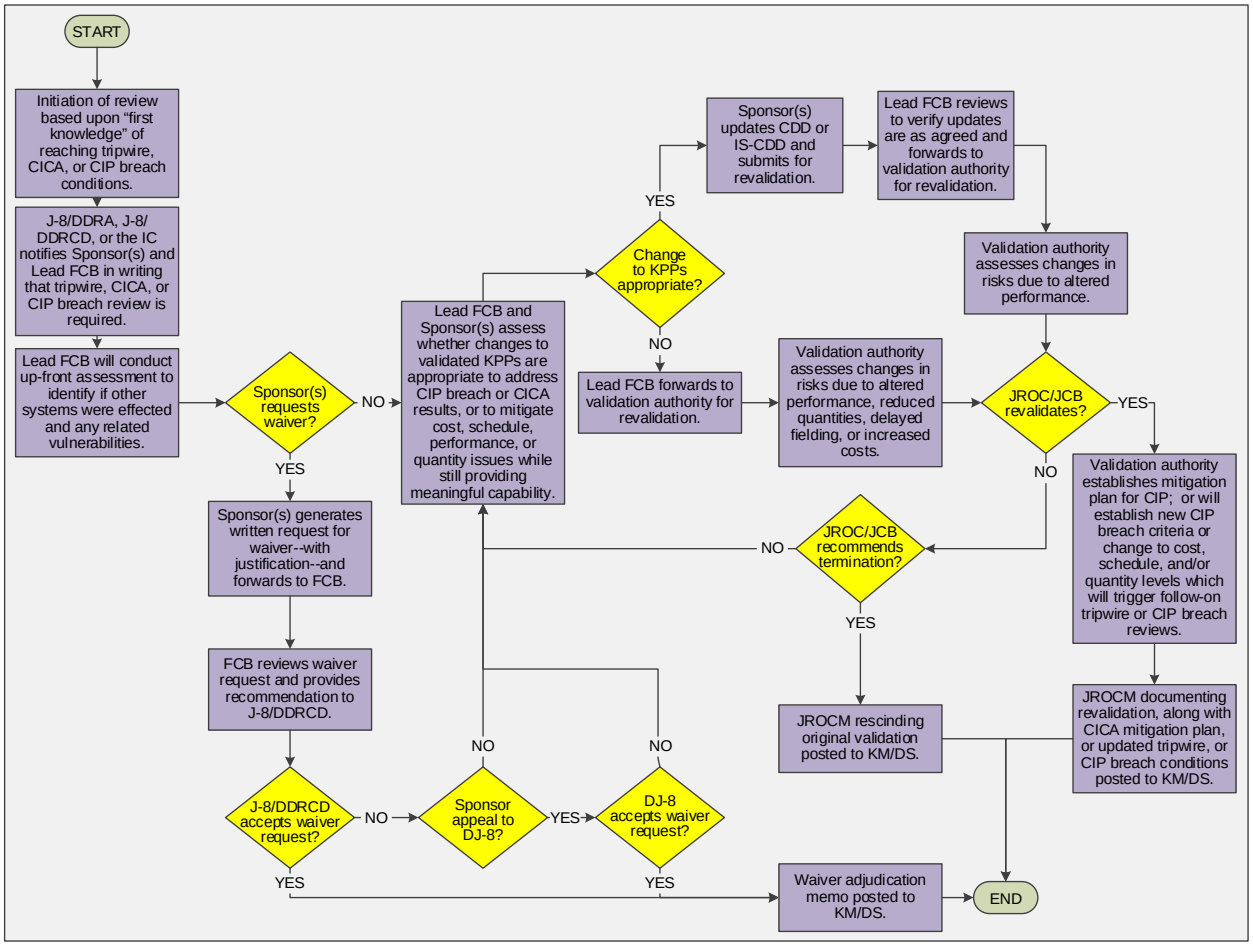

Figure A- 12: JROC/JCB Tripwire, CICA and CIP Breach Review Process

3.4.2. JROC or JCB Tripwire Reviews.

3.4.2.1. J-8/CAD or J-8/PBAD initiates a JROC/JCB Tripwire review based on "first knowledge" of program costs, schedule, and/or quantity changes reaching the trigger values outlined in the validation JROCM and providing notification to the Joint Staff J-8, Deputy Director for Resources and Acquisition (J-8/DDRA). The J-8/DDRA will notify the Sponsor and the Lead FCB that trigger conditions have been met and that a JROC/JCB Tripwire review is required. First knowledge of a trigger condition is usually determined by, but not limited to, one of the following events:

3.4.2.2. POM or Budget Reviews.

3.4.2.3. Program restructures.

3.4.2.4. JCIDS Reviews.

3.4.2.5. Defense Acquisition Executive Summary (DAES) Reviews.

3.4.2.6. Overarching Integrated Process Teams (OIPTs).

3.4.2.7. Selected Acquisition Reports (SARs).

3.4.2.7.1. Program Deviation Reports or changes to APBs.

3.4.3. CICA. The IC or Original Classification Authority (OCA) will identify compromise and conduct a damage assessment. The Damage Assessment Report (DAR) will be submitted to DJ-8 who will notify J-8/DDRCD. J-8/DDRCD will assess DAR and identify/assign FCBs. Lead FCB will coordinate with Service/Sponsor to further assess DAR, make any additional notifications (Requirements Managers/Program Managers/etc.), and develop mitigation plan. FCBs will provide recommended mitigation plan to JCB/JROC and will monitor progress towards mitigation activities. Potential mitigation actions could include changes to:

3.4.3.1. KPPs/KSAs/APAs.

3.4.3.2. Updates to CIPs.

3.4.3.3. DOTmLPF-P Changes.

3.4.3.4. Service TTPs.

3.4.4. CIP Breach Reviews. The supporting Service Intelligence center initiates the CIP breach and notifies the DJ8, the appropriate DoD offices, the affected program office(s). DJ8 will notify J-8 DDRCD who will notify the affected FCB(s).

3.4.4.1. CIP Breach Reviews are based on validated KPPs that are critical to the development of an effective military capability.

3.4.5. Review Process.

3.4.5.1. For CICA or CIP Breach Reviews, the Lead FCB, together with other stakeholders involved in the review, will conduct an up-front assessment to identify whether there are other systems in their portfolio that were affected either due to a CIP breach caused by a foreign entity's demonstrated threat capability or due to program information loss.

3.4.5.2. The Lead FCB will work with the Sponsor(s) to assess whether an adjustment to validated performance attributes (KPPs, KSAs or APAs) is appropriate to mitigate the tripwire, compromise or breach conditions.

3.4.5.2.1. A key aspect of this review is a robust understanding of the impact on UJTs enabled by the capability solution and impact on critical enablers/dependencies. Discussions and briefings related to the review will include impacts to both the program under review as well as other impacted programs within and across the portfolios.

3.4.5.2.2. This understanding of impacts is facilitated by review of the applicable DoDAF OVs, CVs, and SVs; this includes the OV-5a (UJTs), CV-3 (time-sequenced capability requirements), and SV-8 (time sequenced dependencies/enablers).

3.4.5.3. In cases where adjustment of a validated JPR is appropriate to address the tripwire, the Sponsor will submit via the Joint Staff Gatekeeper for

revalidation. The Lead FCB will forward the change request to the JCB and/or JROC for review and revalidation.

3.4.5.4. In cases where adjustment of performance attributes (KPPs, KSA or APA) cannot mitigate the tripwire, classified information compromises, or breach conditions, the validation authority will re-evaluate the operational risks associated with the delayed and/or decreased capabilities offered by the program and consider whether any alternatives are more appropriate to satisfy the original capability requirements.

3.4.5.5. The validation authority will assess the potential impact on other capability solutions that are dependent on or enablers for the capability solution under JROC/JCB Tripwire review and resulting changes to operational risk.

3.4.5.5.1. If revalidated, the validation authority will also establish new program costs, schedule, and/or quantity levels which will trigger follow-on JROC/JCB Tripwire reviews if the program experiences further changes.

3.4.5.5.2. If not revalidated, the validation authority will recommend the Sponsor and Lead FCB consider alternate approaches to mitigation.

3.4.5.6. Elapsed time between written notice and final adjudication by the validation authority will not exceed 75 calendar days.

3.4.6. Waiver. The Sponsor may submit a written request to the FCB for relief if they do not believe the JROC/JCB Tripwire, CICA, or CIP breach is necessary.

3.4.6.1. The FCB will review the Sponsor's justification and provide a recommended disposition to the J-8/DDRCD.

3.4.6.2. If J-8/DDRCD, as the approval authority, does not approve the request, the Sponsor may appeal to DJ-8 for final decision.

3.4.6.3. If approved, a waiver memorandum is retained in the KM/DS system. If not approved, the FCB review begins within 30 calendar days.

3.4.7. Other review authority. JROC/JCB Tripwire, CICA, and CIP breach reviews do not preclude a validation authority from requiring a review of validated requirements or programs by directly communicating to the applicable Sponsor and requesting a review.

3.4.7.1. The JROC and JCB issue review notification via JROCM.

3.4.7.2. The J-8/DDRCD issues review notification via memorandum.

3.4.7.3. Other independent validation authorities are not required to have similar review procedures but may issue similar review notifications IAW their internal processes.

3.5. Staffing of Nunn-McCurdy Unit Cost Breach.

3.5.1. Statutory basis. These reviews of acquisition programs are required by statute, as outlined in Reference [19]

3.5.2. Nunn-McCurdy Unit Cost Breach reviews are initiated:

3.5.2.1. When MDAPs experience cost growth of 15 percent from their current baseline or 30 percent from their original baseline, they are in a “significant” Nunn-McCurdy Unit Cost Breach. Sponsors must notify Congress within 45 calendar days after the report (normally program deviation report) upon which the determination is based. Sponsors must also submit a SAR with the required additional unit cost breach information.

3.5.2.2. When MDAPs experience cost growth of 25 percent from their current baseline or 50 percent from their original baseline, they are in a “critical” Nunn-McCurdy Unit Cost Breach. Programs in “critical” breach status are subject to detailed review for potential termination.

3.5.3. Review teams. USD (A&S) organizes integrated process teams (IPTs) to assess national security impact, analyze alternatives, estimate lifecycle costs and review management structure. More detail on Nunn-McCurdy Unit Cost Breach procedures are in Reference [5].

3.5.4. JROC participation. The JROC and its subordinate boards participate in these reviews in order to review the relevant capability requirements, associated capability gaps, and operational risks, and provide recommendations with respect to the essentiality of the program to satisfying capability requirements that are critical to national security.

3.5.4.1. Upon notification by the Joint Staff Gatekeeper of a Nunn-McCurdy Unit Cost Breach, the lead (and supporting, if necessary) FCB, together with other stakeholders involved in the review, will initiate a review of their capability requirements portfolios to assess the impact of the program in question upon capability requirement(s) in their capability requirements portfolio.

3.5.4.2. Focus of the reviews must be on the essentiality of the program to satisfying capability requirements that are critical to national security. This part of the review should begin with examination of the DoDAF OV-5a (UJTs) and CV-3 (time sequenced capability requirements) associated with the program and comparison to similar capabilities within the capability requirements portfolio. Alternative CONOPS or alternative capability solutions should also be considered.

3.5.4.3. As time will have passed since the validation of the original capability requirements upon which the program was established, review of strategic guidance, DIA- or Service-approved threat products, and/or other aspects of operational context may be necessary before evaluating the essentiality of the program.

3.6. Tailored staffing of Other Reviews or Issues.

3.6.1. Any other requirements related reviews or issues to be considered by the JROC or subordinate boards may use variations of the basic staffing process.

3.6.2. Tailoring of the staffing process or adaptation of alternative staffing processes for issues or reviews not specifically outlined above are at the discretion of the Joint Staff Gatekeeper.

3.6.3. Annual/Biennial FCB Review for IS programs. For all IS programs with a valid IS-ICD, the Sponsor shall provide the Lead FCB an update a year following the validation and then biennially after. For an IS-CDD, the Sponsor shall provide the Lead FCB an update every second year following the validation. The Lead FCB will determine if the JROC or JCB should review the following items and will make appropriate recommendations for action.

3.6.3.1. Progress in delivering capability solutions within the required timeframe and available funding.

3.6.3.2. Compliance with the applicable Enterprise Architecture and data standards.

3.6.3.3. Other items identified by the IS-ICD or IS-CDD validation.

APPENDIX B TO ENCLOSURE A
JCIDS URGENT/EMERGENT PROCESS

1. Overview.

1.1. Purpose. The urgent/emergent staffing process is designed to provide Requirements Sponsors timely review and validation of proposed capability requirements related to ongoing or anticipated contingency operations which, if not satisfied in an expedited manner, would result in unacceptable loss of life or critical mission failure. Solution Sponsors have 2 years to field a capability solution in the urgent/emergent process.

1.1.1. This appendix provides the overview of the urgent/emergent staffing processes for JUONs and JEONs in support of urgent capability acquisition of capability solutions, including those potentially addressed by non-materiel solutions and service contracting efforts.

1.1.2. DoD Component UONs are reviewed and validated by a DoD Component (Services exercise independent validation authority for Component-specific urgent needs), IAW References [17], [20], [21], [22], [23], [24], and [25]. Within 14 days of DoD Component validation, the Requirements Sponsor shall provide a copy of the final validated DoD Component UONs to the Joint Staff Gatekeeper for information and visibility into capability requirements portfolios managed IAW Enclosure C of this manual.

1.1.3. Joint warfighter issues, including the acquisition of materiel capability solutions in response to validated capability requirements, are addressed IAW Reference [26].

1.2. Applicability. This appendix applies to the Joint Staff, Services, CCMDs, and other DoD organizations. JUONs, JEONs, and DoD Component UONs are appropriate for the following:

1.2.1. Capability requirements that will have an initial capability solution fielded within 2 years. Requirements Sponsors must be able to affirmatively answer the following questions:

1.2.2. JUONs. Are the capabilities being driven by on-going contingency operations necessary to prevent loss of life or critical mission failure, and if so, do they require out-of-cycle funding to initiate program execution.

1.2.3. JEONs. Are the capabilities that are driven by anticipated contingency operations necessary to prevent loss of life or critical mission failure, and if so, do they require out-of-cycle funding to initiate program execution.

1.3. Proponent. The proponent for this appendix is the J-8/JCD. For questions, contact J-8/JCD at (703) 695-2705.

2. JCIDS Urgent/Emergent Process.

2.1. JCIDS Urgent/Emergent Needs. The review and validation process for JUONs, JEONs, and DoD Component UONs emphasizes speed to enable approaches that rapidly deliver capability solutions to the joint warfighter for an ongoing or anticipated contingency operation.

2.1.1. The review may not be as robust as deliberate staffing and therefore adjustments may be made to enable rapid delivery of capability solutions, but every effort will still be made to avoid validation of a sub-optimal set of requirements resulting from the expeditious review. Reassessment of the JUON, JEON, or DoD Component UON will be required if there is a plan to extend the capability or a plan to transition it into a long-term enduring capability.

2.1.2. The capability solution fielded in response to a JUON, JEON, or DoD Component UON, may not fully satisfy the validated requirements. Compromises may be made in areas such as price, interoperability, sustainability, training, etc. In cases where urgent/emergent capability requirements are proposed for extension or validation as enduring capability requirements, the enduring capability solution may not be the same as the rapidly fielded solution.

2.1.3. Requests for acceleration or extension to staffing timelines may be submitted to the Joint Staff Gatekeeper on a case-by-case basis.

2.1.4. A Requirements Sponsor may withdraw a document from staffing at any time after submission and acceptance of the document for further evaluation. The Requirements Sponsor will notify the Joint Staff Gatekeeper and request return of the document.

2.2. JCIDS Interaction with Urgent Capability Acquisition. Figure A-13 depicts the interaction between JCIDS and the Urgent Capability Acquisition Process. Once validated, JUONs, JEONs, and DoD Component UONs allow initiation of urgent capability acquisition activities to develop and implement capability solutions in a shorter timeframe than typical of deliberate DAS processes. These urgent capability acquisition activities may also include expedited procurement of Commercial Off-the-Shelf (COTS), Government Off-the-Shelf (GOTS), and/or Non-Developmental Item (NDI) solutions, or modification/acceleration of ongoing development programs initiated under the deliberate process. Urgent capability acquisition in response to validated JUONs, JEONs, and DoD Component UONs will be accomplished IAW References [5] and [26].

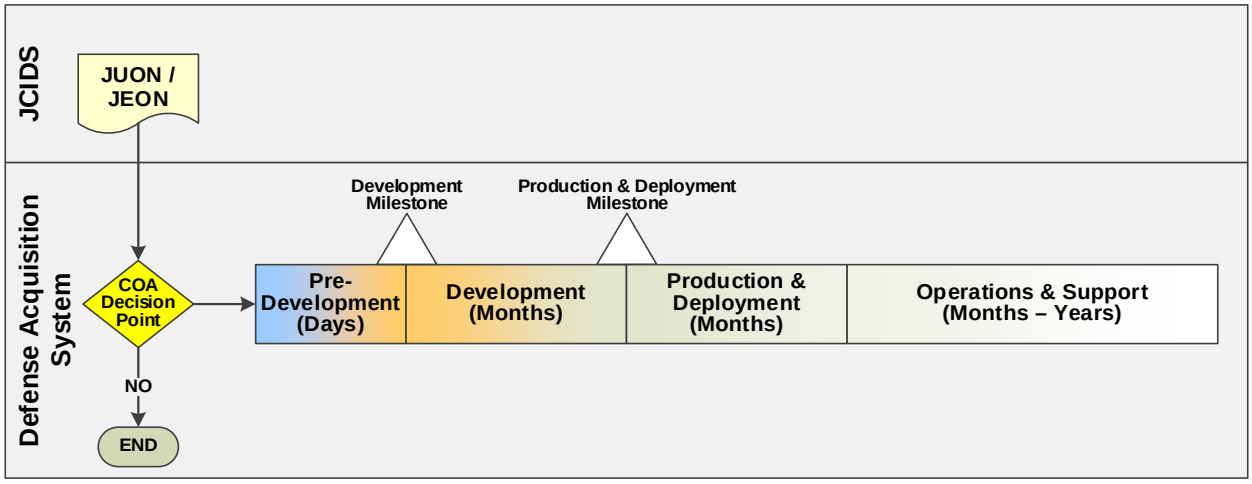

Figure A- 13: Interaction of JCIDS Urgent/Emergent Path and Urgent Capability Acquisition Process

3. JCIDS Urgent/Emergent Staffing.

3.1. JUON Validation. Figure A-14 presents the JUON Staffing timeline. JUON staffing takes no more than 15 days; 1 day for the Joint Staff Gatekeeper to assign a Lead FCB for triage, and 14 days for the FCB to conduct triage and present a validation recommendation to the validating authority. Exigent circumstances may require more expeditious staffing to assess a potential solution.

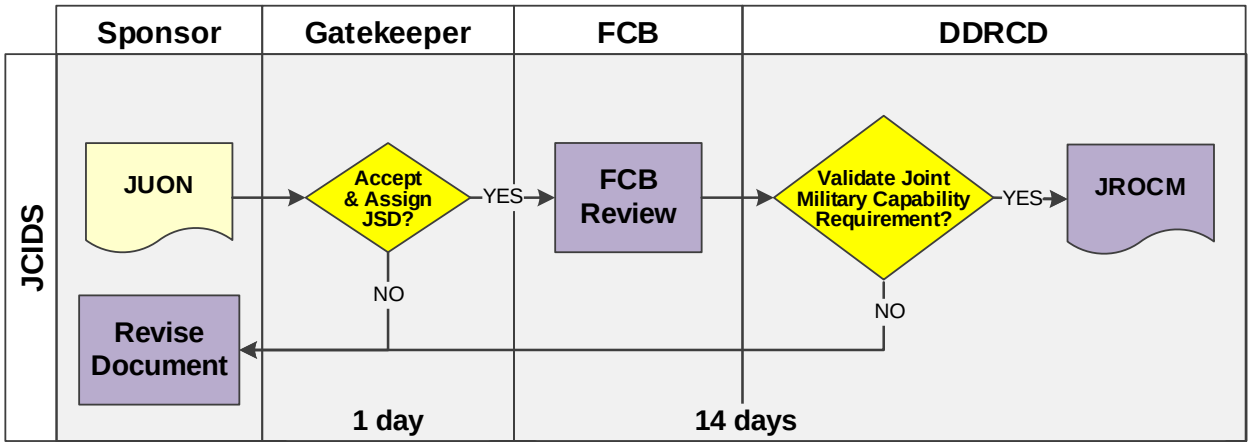

Figure A- 14: JUON Staffing (15 days)

3.2. JEON Validation. Figure A-15 presents the JEON Staffing timeline. JEON staffing takes no longer than 31 days upon receipt of VCJCS approval to enter the emergent lane of JCIDS. This includes 1 day for the Joint Staff Gatekeeper to assign a Lead FCB for review and 30 days for the FCB to conduct review, prepare a recommendation, and schedule the JCB. The JCB or JROC is the approval authority for JEONs.

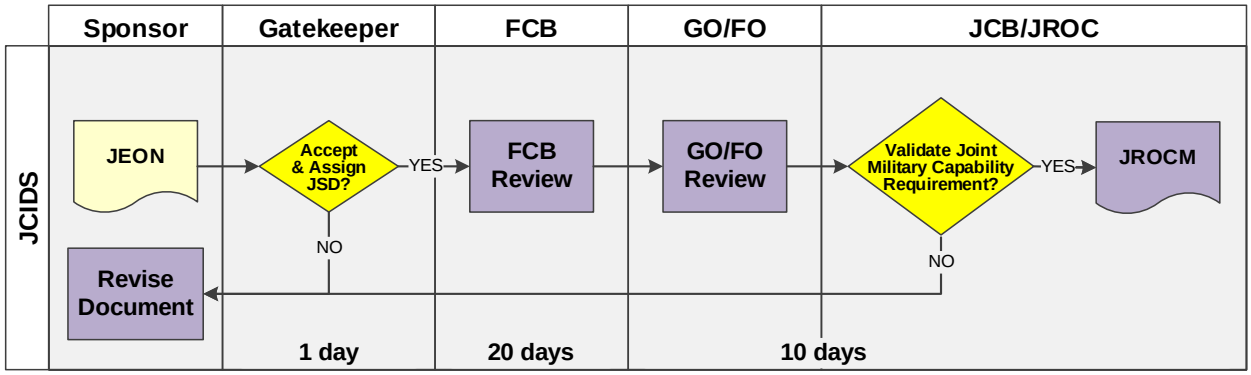

Figure A- 15: JEON Staffing (31 days)

3.3. Staffing Process.

3.3.1. Initiation. The Requirements Sponsor provides the JUON and JEON to the Joint Staff Gatekeeper and to the Director, JRAC for initial screening and review. Staffing begins when the Joint Staff Gatekeeper submits the document from the Requirements Sponsor into JCIDS. All documents undergoing staffing are considered "draft" until validated by the appropriate validating authority.

3.3.2. Joint Staff Gatekeeper Review. The Joint Staff Gatekeeper has 1 day to perform initial screening and review in order to determine if the entry criteria has been met. At the end of the 1-day period, the Joint Staff Gatekeeper must either return the document to the Requirements Sponsor with the rationale for doing so, or submit it into JCIDS for staffing consideration.

3.3.2.1. Once the JUON is submitted for staffing, it is then assigned directly to a Lead FCB and JRAC for collaborative review.

3.3.2.2. JEONs are first confirmed by the VCJCS, via the Joint Staff Gatekeeper and DJ-8, due to the unique nature of capability requirements associated with anticipated contingency operations. Once the VCJCS provides confirmation that the JEON may use the emergent process, JEONs are assigned to a Lead FCB and JRAC for collaborative review.

3.3.2.3. The Joint Staff Gatekeeper can modify the staffing timeline of the document when circumstances arise that require it.

3.3.3. FCB Review. The Lead FCB, in collaboration with JRAC, will assess the validity of the JUON or JEON and identify potential approaches to the solution that could satisfy the capability requirements in the requested timeframe.

3.3.3.1. The first assessment for JUONs and JEONs is the identification of the drive of the change that necessitates the urgent or emergent need. For example, what has changed in strategic guidance, the global context, threats, and/or ongoing or anticipated contingency operations, which now requires a different action than approved in the Service POMs, previous requirements, and acquisition decisions?

3.3.3.2. Use of JUONs and JEONs is limited to circumstances that mandate their use. JUONs and JEONs are used ONLY when other means of addressing the need are not practical for satisfying the capability requirements in the operational timelines. The Lead FCB will assess whether there are any timelier approaches to address the urgent or emergent need in place of pursuing a new capability solution.

3.3.3.3. During this review, the Lead FCB and JRAC will consider COTS/GOTS/NDI solutions as well as the potential to deploy early prototypes from ongoing acquisition programs or Science and Technology (S&T) efforts as a rapid means to address the JUON or JEON.

3.3.3.4. The Lead FCB and JRAC will identify any related JUONs, JEONs, ICDs, IS-ICDs, CDDs, and IS-CDDs that may be related to the JUON or JEON under review.

3.3.3.5. Identification of a potential solution is a desired outcome to assist in cost and schedule estimations. Staffing a JUON or JEON will not be delayed to assess potential solutions.

3.3.3.6. At the end of their assessment, the Chair of the Lead FCB, along with a representative from JRAC, makes a recommendation to the validation authority on whether to validate the JUON or JEON. If applicable, recommended solutions are also provided to the validation authority.

3.3.4. Validation Authority.

3.3.4.1. The J-8/DDRCD is the validation authority for JUONs.

3.3.4.2. The JROC, or JCB if designated by the VCJCS, is the validation authority for JEONs.

3.3.5. Validation Decision.

3.3.5.1. The validation decision is based on whether the JUON or JEON meets the definitions detailed in this section. The validation authority must consider the following:

3.3.5.1.1. The operational timeframe, risk, and likely impact on mission success and/or impact on the safety of forces that would justify validation of the capability requirements and associated capability gaps presented in the JUON or JEON.

3.3.5.1.2. Whether the capability requirements and proposed timeline for fielding capability solutions meet the urgent/emergent needs of the CCMD(s).

3.3.5.1.3. Whether the capability requirements are prioritized higher than all non-urgent/emergent capability requirements.

3.3.5.1.4. Whether the capability requirements represent unnecessary redundancy in capabilities across the joint force.

3.3.5.1.5. If estimated resource levels satisfy the capability requirements and are consistent with the priority of the capability requirements.

3.3.5.2. The validation authority will make one of the following decisions:

3.3.5.2.1. Validate the JUON or JEON. Following validation of the JUON or JEON, JRAC will designate a Solution Sponsor to rapidly fund, develop, acquire, field, and sustain a capability solution IAW Reference [26].

3.3.5.2.2. Validate part of the JUON or JEON. If it is determined that the Requirements Sponsor's capability requirement is best validated through a mix of urgent and deliberate requirements validation processes, the validation authority will validate part of the capability requirement as a JUON or JEON, and recommend the Requirements Sponsor re-submit the remainder of the capability requirement for validation in the deliberate requirements validation process. The validation authority can also recommend that the Requirements Sponsor re-submit their need into other processes such as the Global Force Management (GFM) process or JMVP.

3.3.5.2.3. Reject the JUON or JEON.

3.3.5.2.3.1. Reasons for rejection include, but are not limited to:

3.3.5.2.3.1.1. If it is anticipated that technology challenges or other issues would prohibit the fielding of a militarily useful solution in the operational timeline given.

3.3.5.2.3.1.2. If the validation authority determines that the criteria for being a JUON or JEON are not met.

3.3.5.2.3.2. The validation authority will return the JUON or JEON document and provide the Requirements Sponsor with the reasons for doing so, along with a recommendation that the Requirements Sponsor accept risk, adopt a non-materiel approach, or pursue the capability requirement through the deliberate requirements validation process or other processes (GFM process, JMVP, etc.).

3.3.6. Validation Duration.

3.3.6.1. Validated JUONs and JEONs remain valid for the timeframe and scope articulated in the original JUON or JEON unless withdrawn by the Requirements Sponsor, revoked by the validation authority, or an enduring capability requirement is validated in support of transition of a rapidly fielded capability solution to an enduring POR.

3.3.6.2. Limits on the continuing validity of DoD Component UONs are at the discretion of the DoD Component validation authority.

3.3.7. Validation Documentation.

3.3.7.1. Validated capability requirements are communicated from the validation authority to the Director, JRAC, via a J-8/DDRCD validation memorandum for JUONs or JROCM for JEONs.

3.3.7.2. Validation documentation needs to include whether or not the capability requirement(s) are partial or fully validated.

If the JUON or JEON is not validated, the validation authority sends a memorandum to the Requirements Sponsor.

3.3.7.3. Validation decisions will be uploaded to the KM/DS system for archival purposes.

3.3.7.4. Any changes proposed by the Requirements Sponsor which relate directly to the substance of the validation - performance, lifecycle cost, schedule, and/or quantity – will be coordinated with the validation authority to determine the required level of review for revalidation by the validation authority.

3.3.7.5. The validation authority may rescind a previous validation and/or direct changes to or re-staffing of a validated document at any time. The validation authority will notify the Requirements Sponsor in writing, with rationale for the rescission.

3.4. Modifications to Validated JUONs and JEONs.

3.4.1. Modification Review. Upon notification from the Joint Staff Gatekeeper of a proposed modification to a validated JUON or JEON, the Lead FCB, in coordination with JRAC, will review the proposed changes.

3.4.2. Validation Recommendation. The Lead FCB, in coordination with JRAC, will make a validation recommendation to the validation authority.

3.4.3. Validation Decision. The validation authority will generate a memorandum either validating the modifications to the JUON or JEON, or documenting the decision to not validate the modifications.

3.5. Periodic Validation Reviews.

3.5.1. Quarterly Review. The Joint Staff Gatekeeper, together with the JRAC, reviews validated JUONs and JEONs quarterly to assess progress toward fielding capability solutions in a timely manner. Similar reviews of validated DoD Component UONs are at the discretion of the DoD Component validation authority. These reviews are briefed to the Warfighter Senior Integration Group (W-SIG) for OSD, JS, and CCMD customer oversight.

3.5.2. Biennial Review. The validation authority reviews validated JUONs and JEONs 2 years after the validation date, unless withdrawn earlier by the validation authority or Requirements Sponsor. Reasons for withdrawal may include an assessment of the solution's limited duration or a proposal to transition the rapidly fielded capability solution to the deliberate acquisition process where appropriate. This ensures that the urgent capability requirements remain valid. Similar reviews of validated DoD Component UONs are at the discretion of the DoD Component validation authority.

3.5.2.1. The Joint Staff Gatekeeper, along with JRAC and the W-SIG, will communicate with the CCMD and the Solution Sponsor to see if the capability solution is working, whether the capability requirement needs to be changed, or if there is more development needed to produce a suitable capability solution.

3.5.2.2. In cases where a JUON or JEON was validated and technology development took longer than 2 years, the FCB and JRAC will assess whether continued development of the capability solution would be more effectively accomplished if it were transitioned over to an enduring requirement validated through the deliberate requirements and acquisition processes.

3.5.2.2.1. If a JUON or JEON is not making satisfactory progress toward a capability solution for technology development reasons, a recommendation for withdrawal of the JUON or JEON validation may be initiated by the Requirements Sponsor, JRAC, or validation authority.

3.5.2.2.2. Where appropriate, the withdrawal of the validation by the validation authority will include a mutually agreed to recommendation for an appropriate point in the deliberate process to initiate a deliberate development effort.

3.5.2.3. This review also serves as a driver to determine if validation of enduring capability requirements and transition of a successfully fielded capability solution to an enduring POR is appropriate, if not already initiated by the Requirements Sponsor.

4. Assessment of Operational Utility.

4.1. Timing. For any rapidly fielded capability solution delivered to operational users in response to a JUON or JEON, the original Requirements Sponsor will generate an assessment of the capability solution no later than six months after initial delivery to facilitate transition, sustainment, or alternate approaches.

4.2. Requirement Sponsors are responsible for resourcing the assessment of the capability solution.

4.3. Intent. The assessment is intended to be brief and provide feedback against the original capability requirements submitted in the JUON or JEON. These assessments are specifically intended to inform the validation authority to support the decision-making process with respect to:

4.3.1. Making timely changes, where appropriate, to capability requirements validated in JUONs and JEONs, or rescinding the validation of a capability requirement when no longer required by the original Requirements Sponsor.

4.3.2. To support the decision as to whether or not to transition a rapidly fielded capability solution to an enduring POR when deemed by the validation authority to be of best interest to the Joint Force.

4.4. Tailorability.

4.4.1. The assessment may also document applicable shortcomings in the fielded capability solution and any improvements to be made in the future. It does not limit the ability of the Solution Sponsor to provide more in-depth operational testing and assessment as part of acquisition efforts, and does not relieve the Program Manager (PM) from conducting acquisition assessments IAW Reference [5].

4.4.2. The validation authority may waive the assessment or specify alternative measures if it is determined that the assessment of operational utility is not practical due to capabilities not being fielded to the user or due to insufficient quantities being delivered in the first six months.

4.5. Disposition. To provide authoritative disposition of rapidly fielded capability solutions, any assessments recommending enduring capability requirements will be endorsed by the original authorizing official (CCMD Commander, Deputy Commander, or Chief of Staff), reviewed by the FCB WG or FCB, and validated by the appropriate validation authority as determined by the Joint Staff Gatekeeper.

4.5.1. For recommendations to transition JUONs or JEONs to enduring capability requirements, the FCB Chair and other stakeholders will evaluate the impact of the transition to the capability requirements portfolio and the priorities of related capabilities.

4.5.1.1. Note that the transition recommendation is with respect to capability requirements and might not result in long-term sustainment of the rapidly fielded system if a more appropriate and cost-effective replacement can be used.

4.5.1.2. The FCB may provide recommendations to the validation authority for transition to an enduring capability requirement even when the original authorizing official does not recommend it, when such a recommendation is in the interest of managing the capability requirements portfolio.

4.5.2. Once determined that the transition will happen, the Requirements Sponsor will consider the need to generate a CDD, DCR, or other appropriate documentation for validation to identify the performance attributes, DOTmLPF-P considerations, and supporting information for the balance of development, fielding, and required sustainment to meet the follow-on enduring capability solution. This will be in-sync with the MDA's direction to the Solution Sponsor via an ADM to transition the rapidly acquired solution into a POR.

4.5.3. The validated JUON or JEON and related assessment of operational utility should be leveraged to minimize the required effort to generate JCIDS documents for follow-on efforts.

4.5.4. Proposals to validate enduring capability requirements and transition a capability solution to a POR must also include an appropriate level of follow-on analysis to ensure that the capability requirements are set appropriately, given

an enduring rather than urgent/emergent timeframe, and that the rapidly fielded capability solution remains the most appropriate alternative for enduring use and sustainment. While some level of assessment was likely performed in support of the rapid acquisition decisions, the timeliness of a solution may have carried greater weight than the lifecycle cost or other evaluation factors typical of the deliberate requirements and acquisition processes. In addition, an assessment must be made to ensure that normal acquisition activities and considerations, potentially omitted for expediency in rapid acquisition, are addressed in the validation of enduring capability requirements and planning for transition of a rapidly fielded capability solution to a POR.

4.6. Archiving: Upon completion, the assessment is posted to the KM/DS studies repository to facilitate sustainment and follow-on efforts.

4.7. Assessment Content. An assessment of operational utility will be documented in memo format and consist of the following sections:

4.7.1. Header info. Date, original requirement/source document and validation date, assessing organization (Requirements Sponsor), Point of Contact (POC) info, capability solution being assessed, solution organization (Solution Sponsor), POC info, etc.

4.7.2. Assessment period. Identify initial date capability solution was first provided to the end user and length of time upon which the assessment is based. It is mandatory that the Requirements Sponsor provide the assessment results back to the Joint Staff Gatekeeper within six months after initial fielding. An assessment may be submitted in a shorter timeframe in situations where it is quickly determined that the capability solution does not deliver the required operational utility. If the Requirements Sponsor cannot meet the six-month deadline, they must submit reasons for delay to the Joint Staff Gatekeeper.

4.7.3. Conclusion. The three categories for the conclusion are:

4.7.3.1. Failure/Limited Success.

4.7.3.1.1. The fielded capability solution does not provide operational utility satisfying the capability requirements in the validated JUON or JEON. In the assessment, the Requirements Sponsor also provides confirmation that the originally requested and validated capability requirements are still appropriate or identifies any necessary changes for revalidation.

4.7.3.1.2. The validated JUON or JEON does not need to re-enter staffing and validation unless the capability requirement changes. For unchanged capability requirements, the JRAC and Solution Sponsor will leverage the original validated JUON or JEON to generate a new funding and fielding plan and develop an alternate capability solution as soon as possible.

4.7.3.2. Success/Limited Duration Requirement.

4.7.3.2.1. The capability solution satisfies the urgent/emergent capability requirement for the limited duration purposes identified in the validated JUON or JEON.

4.7.3.2.2. No reassessment of the capability requirements or capability requirements portfolio is required, and the Solution Sponsor will sustain the capability solution for the duration of the validated timeframe and then dispose of the capability solution.

4.7.3.3. Success/Enduring Requirement.

4.7.3.3.1. The capability solution satisfies the urgent/emergent capability requirement for the limited duration purposes identified in the validated JUON or JEON, but also provides enduring capabilities that should remain in the joint force.

4.7.3.3.2. For assessments documenting operational utility and an enduring requirement for the rapidly fielded capability solution, the Solution Sponsor will continue to sustain the rapidly fielded capability solution until replaced by an alternative capability solution, if applicable.

4.7.4. Required Capability/Performance. State “meets all required capabilities” for a completely successful capability solution. If it does not deliver all required capabilities, then identify all shortfalls, limitations, and/or issues with each required capability. Be as specific as possible to better inform further development activities or alternative approaches for delivering the required capabilities.

4.7.5. Changes to CONOPS, Mission(s), and/or Threat(s). If the capability solutions end up being used exactly as proposed, then state “None” under this section. Identify if changes were made due to either the nature of the capability solution or to innovations since the capability was fielded and include how the capability solution is being used. Provide details that can be used to assist in sustainment and/or further development of the capability solution, as well as provide any detail to support validation of enduring capability requirements and transition of capability solutions to a POR when appropriate. (Note that if changes to threat and/or usage drive significant changes to the required capabilities, an update and revalidation of the JUON or JEON may be required.)

4.7.6. Changes to required quantities. If the capability solutions end up being used exactly as proposed in the original JUON or JEON, then simply state “Same as identified in JUON or JEON.” If the capability solution has operational utility in a broader sense than originally anticipated or is being consumed at a greater rate or over a longer period, provide updated estimates of required quantities. (Note that if significant changes are made to the required quantities, an update and revalidation of the JUON or JEON may be required.)

4.7.7. Changes to anticipated sustainment duration. For capability solutions which end up being used exactly as proposed in the original JUON or JEON simply state "Same as identified in JUON or JEON." If the capability solution has operational utility in the contingency in a broader sense or longer duration than originally anticipated, provide details of anticipated sustainment timeframe. (Align with quantities above, if consumption/attrition is expected to be an issue over the expanded timeframe.)

4.7.8. Other issues/considerations. Identify any other issues that affect the utility and/or sustainment of the capability solution. Issues may include, but are not limited to, fielding, training, reliability/maintainability, interoperability, system security, proprietary software and licensing concerns, etc.

4.7.9. Additional opportunities. If the fielded capability solution, or derivatives thereof, is anticipated to provide operational utility to other parts of the joint force, outline any identified opportunities.

4.7.10. Testing data. If any formal or informal testing/evaluation was performed on the capability solution during the assessment period, provide a summary of testing and results. If any follow-on testing is planned, please indicate intended timeframe and scope of testing. Applicable test data and detailed results may be included as an appendix to the assessment. This data can facilitate further refinement/enhancement of the capability solution and provide source data to support proposed validation of enduring capability requirements and support transition of a capability solution to a POR.

4.7.11. Authorized by. Provide release authority's name, rank, and title. Assessments of operational utility must be endorsed by the CCMD Commander, Vice/Deputy Commander, Chief of Staff, or CCMD J-8.

APPENDIX C TO ENCLOSURE A
GATEKEEPING

1. Overview.

1.1. Purpose. The Joint Staff Gatekeeper represents the JROC and has a primary function to ensure that all capability requirements documents provided for initial screening and review are compliant with format and content as appropriate prior to submission for JCIDS staffing of the document for validation. The Joint Staff Gatekeeper manages the overall flow of capability requirements documents, ensures primary stakeholder visibility into documents and issues validated under independent validation authorities, and to provide support to JCIDS activities.

1.2. Applicability. This appendix applies to the Joint Staff Gatekeeper and DoD Component Gatekeepers.

1.2.1. The J-8/DDRCD serves as the Joint Staff Gatekeeper, with most day-to-day activities delegated to the Requirements Management Branch of J-8/JCD.

1.3. Proponent. The proponent for this appendix is J-8/JCD. For questions, contact J-8/JCD at (703) 695-2705.

2. Guidance for Document Submission.

2.1. Single Point of Entry. Sponsors provide all capability requirements documents via their DoD Component Gatekeeper to the Joint Staff Gatekeeper to facilitate single point of entry into the JCIDS process and for submission and determination of the appropriate staffing process and validation authority. Documents received from other entities will be referred back to the DoD Component Gatekeeper prior to staffing.

2.1.1. DoD Component Gatekeepers, with their representatives to the FCB, will assess documents assigned a JSD of Joint Information by the Joint Staff Gatekeeper to determine which documents affect DoD Component equities and require review and commenting.

2.1.2. Capability requirements documents that are validated at the Sponsor level that do not have joint equities must be submitted to the Gatekeeper with a designation of Joint Information within 14 days of Sponsor validation. These documents will be used to provide the FCBs and Joint Staff with visibility into the Sponsor capability portfolios; however, the Joint Staff will not provide comments or validation of these documents.

2.1.3. In cases where minimizing the overall staffing timeline is a priority, Sponsors are encouraged to submit documents for joint staffing of applicable certifications, endorsements, or validation in parallel with any Sponsor approval processes. This ensures that issues from lower level reviews can be addressed between the Sponsor and the Joint Staff before receiving higher level

Sponsor approval and minimizes the need for Sponsor re-approval when addressing joint equities.

2.1.4. Capability requirements documents for capabilities funded by a combination of NIP and MIP funds are submitted to the Joint Staff Gatekeeper to enable a common Gatekeeper function between JCIDS and the Intelligence Community Capability Requirements (ICCR) process.

2.1.4.1. Capabilities funded primarily or wholly with NIP funding, will be developed, reviewed, and validated IAW the ICCR process outlined in Reference [27].

2.1.4.2. Capabilities funded primarily or wholly with MIP funding will be developed, reviewed, and validated under the JCIDS process outlined in this manual.

2.1.5. Documents related to the Defense Business System (DBS) must be submitted by Sponsors to the Joint Staff Gatekeeper to enable a common Gatekeeper function between the JCIDS process and the acquisition of DBS.

2.1.6. DoD Component UONs are not submitted to the Joint Staff Gatekeeper for determination of the appropriate staffing process and validation authority but are submitted for visibility and archiving within 14 days of Component validation.

2.2. Document Submission by Classification Level.

2.2.1. For capability requirements documents and related data classified at or below the level of SECRET, and not protected by ACCM or SAP/SAR:

2.2.1.1. ICDs, IS-ICDs, CDDs, IS-CDDs, and Joint DCRs. Sponsors submit capability requirements documents and related data via the KM/DS system located at the URL in Reference [4]. If a Sponsor wishes to submit a signature page, the Sponsor may submit that one page in pdf format.

2.2.1.2. JUONs and JEONs. Sponsors submit JUONs and JEONs via SIPRNET email or memo to the Joint Staff Gatekeeper without using KM/DS.

2.2.1.3. DoD Component UONs. Within 14 days of DoD Component validation, Sponsors shall submit validated DoD Component UONs via SIPRNET email or memo to the Joint Staff Gatekeeper without using KM/DS.

2.2.2. For capability requirements documents and related data classified above the level of SECRET, and not protected by ACCM or SAP/SAR:

2.2.2.1. ICDs, IS-ICDs, CDDs, IS-CDDs, and Joint DCRs. Sponsors enter placeholder records in the KM/DS system and then provide the capability requirements documents to the Joint Staff Gatekeeper via the Joint Worldwide Intelligence Communications System (JWICS). The placeholder record will include instructions on document location and how to access.

2.2.2.2. JUONs and JEONs. Sponsors submit JUONs and JEONs via JWICS to the Joint Staff Gatekeeper without using KM/DS.

2.2.2.3. DoD Component UONs. Within 14 days of DoD Component validation, Sponsors shall submit validated DoD Component UONs via JWICS to the Joint Staff Gatekeeper without using KM/DS.

2.2.3. For capability requirements documents and related data protected by SAP/SAR:

2.2.3.1. Sponsors or the J-8/SAPCOORD enter a placeholder record in KM/DS only when the presence of the capability requirements protected by SAP/SAR designation can be disclosed at or below the classification level of SECRET. Note that a Reference number or other substitute for the actual title may be used when the presence can be disclosed but the classification of the title is such that it cannot be stored in KM/DS.

2.2.3.2. Capability requirements documents and related data are provided through the Sponsor Special Access Program Control Office (SAPCO) to the J-8/SAPCOORD, who will coordinate with the Joint Staff Gatekeeper for review by appropriately cleared reviewers. To facilitate review of SAP/SAR designated documents, Joint Staff Gatekeeper will:

2.2.3.2.1. Maintain a roster of personnel, appropriately cleared to one or more of the capability requirements portfolios, who can facilitate the review of documents while minimizing the number of additional accesses granted.

2.2.3.2.2. Identify essential JCB or JROC participants who do not have appropriate access to facilitate timely access when/if appropriate.

2.2.3.3. The J-8/SAPCOORD will retain validated documents and associated validation memos IAW SAP/SAR policy outlined in References [28] and [29], and storage and handling procedures for each program.

2.2.4. For capability requirements documents protected by ACCM:

2.2.4.1. Sponsors enter a placeholder record in the KM/DS system only when the presence of the capability requirements protected by ACCM designation can be disclosed at or below the classification level of SECRET.

2.2.4.2. Sponsors coordinate with the Joint Staff Gatekeeper to ensure appropriate personnel are accessed to the ACCM for the review, and that documents are handled IAW the ACCM protections.

2.2.4.3. The Joint Staff Gatekeeper will retain validated documents and associated validation memos in a manner such that only those accessed to the applicable ACCM may review the documents.

2.3. Sequence for Document Submissions.

2.3.1. Concurrent staffing of ICDs and CDDs for the same capability requirement/solution is not allowed.

2.3.2. Submission of a CDD for validation prior to, or in parallel with, the associated post-AoA (or similar study) review is not allowed.

2.3.3. Concurrent staffing of waiver requests for predecessor documents is allowed. The staffing of a successor document will be immediately terminated if the waiver request for its predecessor is denied.

2.4. Waiver Requests.

2.4.1. ICD Waiver Requests. ICDs may be waived by the Joint Staff Gatekeeper, in coordination with the validation authority and MDA, in cases where potential programs are best served by proceeding directly to Milestone A, Milestone B or Milestone C, such as for GOTS/COTS solutions, transitioning JUONs, JEONs, and DoD Component UONs, successful JCTDs, etc.

2.4.1.1. The Sponsor will submit the waiver request in memorandum form to the Joint Staff Gatekeeper. The waiver memorandum must be endorsed by a GO/FO or equivalent authority. The waiver request must include the rationale and justification for why an ICD is not appropriate, the source(s) of equivalent information, and the proposed path forward.

2.4.1.2. The Joint Staff Gatekeeper assigns the waiver request to the appropriate FCBs for evaluation within 10 calendar days of receipt.

2.4.1.3. The Lead FCB will recommend approval or disapproval of the waiver within 13 calendar days.

2.4.1.4. After receiving the recommendation from the Lead FCB, the Joint Staff Gatekeeper will approve or disapprove the request within 10 calendar days.

2.4.1.5. Approval or denial of the request is documented in memo format from the Joint Staff Gatekeeper and is inserted as part of the document to ensure traceability in future st

2.4.2. Other format or process waiver requests. Requests for exceptions or variances to the document formats and processes described in this manual must be directed to the Joint Staff Gatekeeper.

2.4.2.1. The Joint Staff Gatekeeper will work in coordination with the document Sponsor and the appropriate FCB to ensure any exceptions or variances meet the needs of the validation authority while allowing for appropriate flexibility in the capability requirements process.

2.4.2.2. Waivers granted by the Joint Staff Gatekeeper and certification or endorsements by applicable FCBs shall be documented in memo format or KM/DS note and inserted as part of the requirement document or KM/DS file to provide traceability in future staffing and validation activities.

3. Primary Gatekeeping Responsibilities.

3.1. Implement Joint Staff Gatekeeper Activities.

3.1.1. Initial Review. The Joint Staff Gatekeeper provides initial review of all incoming documents and performs the following:

3.1.1.1. Reviews each document submitted, regardless of actual/potential ACAT designation or previous JSD or independent validation authority decisions, to confirm that the document is complete and ready for staffing.

3.1.1.2. Confirms that results of CBAs, studies, and other applicable supporting data for the document have been uploaded to KM/DS.

3.1.1.3. Returns documents of JROC or JCB interest to Sponsors for further development prior to staffing when they are not compliant with the JCIDS formats in this manual. Document rejection prevents initiation of the staffing process until the Sponsor takes corrective actions.

3.1.1.3.1. Documents with discrepancies that are easily corrected will:

3.1.1.3.1.1. Be corrected by the Joint Staff Gatekeeper prior to admitting the document for staffing, or

3.1.1.3.1.2. Be allowed to enter staffing as written, if the discrepancy is a minor formatting error. Joint Staff Gatekeeper noted discrepancies will be documented via Comment Resolution Matric (CRM) in the normal staffing process.

3.2. Conduct Initial Staffing. Once the initial review is approved then the Joint Staff Gatekeeper will:

3.2.1. Identify FCB Assignment. Identifies Lead FCB and supporting FCBs.

3.2.2. Designate JPRs. (The Joint Staff Gatekeeper, on behalf of the JROC, initially designates JPRs during this staffing phase. Final JPR designation will be made by the validation authority when the capability requirements document is validated.)

3.2.2.1. Reviews each of the performance attributes (KPPs, KSAs, and APAs) and those designated by the Sponsor as JPRs. If not determined, all performance attributes designated JPRs will be upgraded to a KPP. The process used by JS Gatekeeper to designate JPRs is listed below:

3.2.2.1.1. Upon initial staffing, Sponsor will recommend whether a KPP should be designated a JPR.

3.2.2.1.2. Joint Staff Gatekeeper will review Sponsor recommendation and the other KPPs, KSAs, and APAs, coordinate with the Lead FCB to receive their recommendation, and will make an initial determination about which performance attributes should be considered for designation as JPRs.

3.2.2.1.3. Figure B-6 in Appendix C of Enclosure B depicts how JPRs will be identified in Section 5 of the CDD.

3.2.2.2. JPR designation will be determined on a case-by-case basis and IAW Reference [2] will be used for those performance attributes considered critical or essential to ensure interoperability, where appropriate, between and among joint military capabilities, and are necessary to fulfill a capability gap(s) of more than one armed force, agency or entity of the DoD.

3.2.2.2.1. The JPR designation is a key criterion used by the Joint Staff Gatekeeper in assigning the appropriate JSD and can be changed at any time in the staffing process.

3.2.2.3. JROC or JCB (depending upon JSD) will validate the entire document but will delegate all non-JPR performance attributes for certification/endorsement authority and change authority to the Sponsor.

3.2.3. Assign JSD. Assigns one of the three possible JSDs (JROC Interest, JCB Interest, or Joint Information) that are based on Joint Warfighter equities.

3.2.3.1. The JSD sets the staffing path and timeline for the document and identifies the validation authority.

3.2.3.2. To maximize speed and flexibility in the JCIDS process, JSDs will be set at the lowest level.

3.2.3.3. JSDs may be changed during staffing but will not be revisited for a subsequent submission of the same document unless the Lead FCB submits a request for JSD change to the Joint Staff Gatekeeper.

3.2.3.4. Subsequent review of previously validated capability requirements documents assigned a JSD of Independent, or Joint integration will be assigned a JSD of Joint Information unless a higher JSD is applicable.

3.2.3.5. With the exception of majority NIP-funded IC capability requirements and requirements managed by the Nuclear Weapons Council (NWC), the JROC may exert validation authority over any capability requirements by changing the JSD to JROC Interest or JCB Interest.

3.2.3.6. There are three JSDs:

3.2.3.6.1. JROC Interest. Applied to capability requirements documents that have performance attributes considered critical or essential to ensure joint interoperability and are necessary to fulfill a capability gap(s) of more than one armed force, agency or entity of the DoD. JROC Interest is used for documents where the intended level of joint oversight cannot be satisfied by assignment of a lower level JSD. The JROC is the validation authority for JROC Interest documents.

3.2.3.6.1.1. Joint military capabilities are the collective capabilities across the joint force, including both joint and force-specific capabilities that are available to conduct military operations requirements.

3.2.3.6.1.2. All capabilities, regardless of JSD, should consider interoperability within the joint force to include joint force enablers.

3.2.3.6.1.3. JROC Interest capability requirements documents will have at least one JPR where the capability requirement has clear joint interoperability or multi-service equities.

3.2.3.6.2. JCB Interest. Applied to capability requirements that have performance attributes considered critical or essential to ensure joint

interoperability and are necessary to fulfill a capability gap(s) of more than one armed force, agency or entity of the DoD. JCB Interest are used for capability requirements documents where the intended level of oversight does not meet the JROC threshold and cannot be satisfied by assignment of a lower level JSD.

3.2.3.6.2.1. The JCB is the validation authority for JCB Interest documents, with the exception of United States Special Operations Command (USSOCOM) or United States Cyber Command (USCYBERCOM) capability requirements documents that have their own Independent Validation Authority for JCB Interest and below documents.

3.2.3.6.2.1.1. USSOCOM validation authority of the combatant commander is under Title 10 U.S.C. § 167a(d)vi.

3.2.3.6.2.1.2. USCYBERCOM validation authority of the combatant commander is under Title 10 U.S.C. § 167b(d)vi.

3.2.3.6.2.1.3. For the purposes of this manual, the term “cyber operations activities” identified in Title 10 U.S.C. § 167b(d)(1) is the functional equivalent of the term “cyberspace operations” as defined in the DOD dictionary and JP 3-12 (R) dated 5 February 2013.

3.2.3.6.2.2. JCB Interest is the minimum JSD for Joint DCRs and for any documents where the Sponsor is a CCMD, with the exception of USSOCOM or USCYBERCOM.

3.2.3.6.2.3. JCB Interest capability requirements documents will have at least one JPR where the capability requirements has clear interoperability or multi-service equities

3.2.3.6.3. Joint Information. Applied to all capability requirements documents that do not need Joint Staff certifications or endorsements and are below the level of JCB Interest. The Sponsor organization has independent validation authority for Joint Information documents and responsibility for applicable certifications and endorsements. Any applicable waivers will be published for visibility. The Service Gatekeeper will be responsible for ensuring timely communication with the Joint Staff Gatekeeper regarding the status of the document and will provide the Joint Staff Gatekeeper a copy of the validated capability requirements document and associated validation memorandum when complete.

3.2.4. Determine Certification or Endorsement Authority. The Certification or Endorsement Authority is determined by the JSD and JPR as shown in Figure A-16, unless otherwise tailored by the Joint Staff Gatekeeper.

Certifications and Endorsements	JROC/JCB Interest or Joint Information[1, 2]	Appendix G to Enclosure B
Net-Ready Certification	Sponsor (or Joint Staff if designated a JPR)	Annex A
FP KPP Certification	Sponsor (or Joint Staff if designated a JPR)	Annex B
SS KPP Endorsement	Sponsor (or Joint Staff if designated a JPR)	Annex C
Sustainment KPP Endorsement	Sponsor (or Joint Staff if designated a JPR)	Annex D
Energy KPP Endorsement	Sponsor (or Joint Staff if designated a JPR)	Annex E
DOTmLPF-P Endorsement	Joint Staff (delegated to Sponsor for all Joint Information documents)	Annex F
Threat Assessment/Intelligence Certification	Joint Staff (delegated to Sponsor for all Joint Information Documents)	Annex G
Weapon Safety Endorsement	Joint Staff (Only applicable for JROC/JCB Interest)	Annex H

Note:
[1] Sponsors have certification and endorsement authority for all performance attributes which are not JPRs. The Joint Staff has certification and endorsement authority for all JPRs.
[2] USSOCOM and USCYBERCOM have certification and endorsement authority for all JPRs in capability requirements documents with a JSD of JCB Interest or below.

Figure A-16: Certification and Endorsement Responsibility

3.2.4.1. Sponsors have certification and endorsement responsibilities for all performance attributes not designated as JPRs regardless of JSD.

3.2.4.1.1. In cases where the Sponsor has authority to certify or endorse and has independent validation authority, the Sponsor organizations will certify/endorse, or waive an item. These actions will be completely at the discretion of the Sponsor.

3.2.4.1.2. In cases where the Sponsor has responsibility for certifications and endorsements, and the JCB or JROC is the validation authority, the Sponsor organizations will certify, endorse, or waive each item, and provide evidence of their applicable certifications or endorsement (which may be incorporated into the Sponsor validation memo) along with their capability requirements document to the Joint Staff Gatekeeper to support staffing and validation.

3.2.4.1.2.1. An example of this is when there are performance attributes (KPPs, KSAs, APAs) that are not designated as JPRs within a JROC or JCB interest CDD.

3.2.4.2. The Joint Staff has certification and endorsement authorities for all JPRs, except those contained in capability requirements documents with a JSD of JCB Interest or below where USSOCOM or USCYBERCOM has validation authority.

3.2.4.3. In cases where Joint Staff certifications or endorsements are required, Sponsors are encouraged to pursue early coordination with the certification or

endorsement authority to ensure document content will be sufficient to obtain the required certification or endorsement, or waiver thereof.

3.2.4.4. Proponent organizations responsible for Joint Staff certifications and endorsements are listed below and information regarding each one is included in Appendix G to Enclosure B of this manual. Joint Staff certifications and endorsements are only required for performance attributes or other characteristics (DOTmLPF-P considerations, intelligence certification, and weapon safety endorsement) in which there are clear joint equites as depicted in Figure A-16.

3.2.4.4.1. Net-Ready Certification. The Chair of the C4/Cyber FCB provides the net-ready certification which is applicable to all IS-ICDs, CDDs, and IS-CDDs.

3.2.4.4.2. Force Protection (FP) KPP Endorsement. The Chair of the Protection FCB provides the FP KPP endorsement which is applicable to all CDDs addressing manned systems, or systems designed to enhance personnel survivability.

3.2.4.4.3. System Survivability (SS) KPP Endorsement. The Chair of the Protection FCB provides the SS KPP endorsement which is applicable to all CDDs and IS-CDDs.

3.2.4.4.4. Sustainment KPP Endorsement. The Chair of the Logistics FCB, in coordination with J-4/MMSD, provides the Sustainment KPP endorsement. The Sustainment KPP endorsement is applicable to all CDDs.

3.2.4.4.5. Energy KPP Endorsement. The Chair of the Logistics FCB, in coordination with J-4/ED and OSD(L&MR), provides the Energy KPP endorsement. The Energy KPP endorsement is applicable to all CDDs and Joint DCRs where the provision of energy, including both fuel and electric power, impacts operational reach or requires protection of energy infrastructure or energy resources in the logistics supply chain.

3.2.4.4.6. DOTmLPF-P Endorsement. The J-7/JIB, in coordination with DOTmLPF-P stakeholder organizations, provides endorsement of DOTmLPF-P considerations and non-materiel capability solutions. The purpose of the DOTmLPF-P content in capability requirements documents is to address non-materiel aspects of a capability requirements recommendation. An ICD or DCR should describe non-materiel approaches that could provide a capability solution which closes or mitigates associated capability gaps. A CDD should describe non-materiel enablers to materiel capability solutions without which the materiel capability solution cannot be successfully fielded DOTmLPF-P considerations pertain to both materiel and non-materiel solutions.

3.2.4.4.7. Threat Assessment/Intelligence Certification. The Joint Staff J-283/Intelligence Requirements Certification Office (J-283/IRCO) provides the intelligence certification including the threat assessment provided by the Defense Intelligence Agency's Technology and Long-Range Analysis Office

(DIA/TLA). The threat assessment and intelligence certification are applicable to ICDs, IS-ICDs, CDDs, IS-CDDs, and Joint DCRs.

3.2.4.4.8. Weapon Safety Endorsement (WSE). The Chair of the Protection FCB provides the WSE which is applicable to CDDs addressing munitions, and Joint DCRs that have an impact on weapon safety.

3.2.5. Initiate staffing of the document. Joint Staff Gatekeeper sends the document to the Lead FCB and ensures notifications generated by KM/DS are sent to all affected stakeholders. Staffing calendars in KM/DS are tentatively set based on nominal process timelines and are updated automatically as process activities are completed.

3.2.5.1. For IC capability requirements assigned to the ICCR process for review and validation, the Joint Staff Gatekeeper will notify the Chair of the BA FCB to enable proper coordination with and participation in the ICCR process.

3.2.5.2. For IC capability requirements assigned to the JCIDS process for review and validation, the Joint Staff Gatekeeper will notify the Associate Director of National Intelligence for Systems and Resource Analysis (ADNI/SRA) to enable proper coordination with and participation in the JCIDS process.

3.2.5.3. For DBS capability requirements, the Joint Staff Gatekeeper will assess if there are equities requiring JCIDS staffing and validation of requirements and notify the applicable FCB(s) and CMO of the decision related to staffing in JCIDS.

3.2.6. Conduct pre-validation activities. Joint Staff Gatekeeper ensures comment adjudication is complete prior to validation of JCB or JROC Interest documents.

3.2.6.1. Comment adjudication unrelated to joint certifications and endorsements must be completed to the satisfaction of the validation authority.

3.2.6.2. A document may be forwarded to the next approval body without completed adjudication to meet specified timelines.

3.2.6.3. Comment adjudication related to joint certifications and endorsements must be completed to the satisfaction of the certifying or endorsing organization. The certification/endorsement or waiver memorandum, will be completed by the certifying/endorsing organization.

3.3. Support Actions for JUONs, JEONs, and DoD Component UONs.

3.3.1. JUONs. Upon receiving a JUON document, the Joint Staff Gatekeeper verifies that the submission meets the JUON criteria as defined in Appendix B of this enclosure.

3.3.1.1. In cases where the submission does not meet the criteria for a JUON, the Joint Staff Gatekeeper will issue a memorandum to the Sponsor and appropriate stakeholders with the rationale for rejection, and if applicable,

suggestion(s) for alternate approaches to satisfy the capability requirement. Disposition will be archived on KM/DS for visibility and reference purposes.

3.3.1.2. In cases where a submission does not meet the criteria for a JUON, but J-8/DDRCD anticipates that VCJCS may approve handling the capability requirement as a JEON, the Joint Staff Gatekeeper will notify the Sponsor of the designation change, and unless withdrawn by the Sponsor, will continue processing the submission as a JEON.

3.3.1.3. Documents meeting the JUON criteria are assigned to the appropriate Lead FCB for collaborative review with the JRAC IAW Appendix B of this enclosure.

3.3.2. JEONs. JEONs require expedited handling in a similar manner to JUONs, but with several distinct differences.

3.3.2.1. Upon receiving a JEON document, the Joint Staff Gatekeeper will coordinate through the Director, Joint Staff J-8 (DJ-8) to the VCJCS to confirm the request justifies expedited handling.

3.3.2.2. In cases where the JEON is not approved by the VCJCS, the Joint Staff Gatekeeper will issue a memo to the Sponsor with the rationale for rejection, and if applicable, suggestion(s) for alternative approaches to satisfy the capability requirement. Disposition will be archived on KM/DS for visibility and reference purposes.

3.3.2.3. Following VCJCS confirmation, JEONs are assigned to the appropriate Lead FCB for collaborative review with the JRAC IAW Appendix B of this enclosure.

3.3.3. DoD Component UONs. DoD Component UONs are validated by DoD Component validation authorities using staffing detailed in References [17], [20], [21], [22], [23], [24], and [25].

3.3.3.1. Joint Staff Gatekeeper will ensure DoD Component UONs are uploaded to KM/DS within 14 days of validation.

3.3.3.2. If a Sponsor also uses processes in References [17], [20], [21], [22], [23], [24], [25], or [30] to manage actions unrelated to documenting urgent or emergent capability requirements and associated capability gaps, they will filter documents accordingly, and upload to KM/DS only those documents which reflect new or modified capability requirements and capability gaps.

3.3.4. Monitoring of validated JUONs and JEONs.

3.3.4.1. The Joint Staff Gatekeeper monitors progress of efforts toward fielding capability solutions for JUONs and JEONs on a quarterly basis IAW this enclosure. The Joint Staff Gatekeeper also initiates reviews of validated JUONs and JEONs that have been active for 2 years or more that have not received an assessment from the Requirements Sponsor indicating limited duration or proposal to transition to a validated enduring capability requirements in support of capability solutions to enduring PORs.

3.3.4.2. The Joint Staff Gatekeeper does not monitor progress of efforts toward fielding capability solutions for DoD Component UONs. However, the validated DoD Component UONs contribute to the capability requirements portfolios managed by the FCBs, and stakeholders in the associated FCB may have interest in the progress of the capability solution.

3.4. Support Actions for Other Submissions.

3.4.1. Study notices and reports.

3.4.1.1. Identify Lead FCB and supporting FCBs as needed to align the study with the appropriate capability requirements portfolios.

3.4.1.2. Ensure the purpose and description of the study are clearly articulated and the supporting documentation is included as part of the KM/DS record.

3.4.1.3. Archive the notice/study in KM/DS and ensure notifications generated by KM/DS are sent to participants including the Sponsor, lead and supporting FCBs, and Service and CCMD representatives.

3.4.2. Post-AoA reviews (or when appropriate analysis such as a Business Case Analysis or Cost-Performance Tradeoff Analysis), JROC/JCB Tripwire reviews, and Nunn-McCurdy Unit Cost Breach reviews.

3.4.2.1. Identify Lead FCB and supporting FCBs as needed.

3.4.2.2. In coordination with J-8/CAD, and J-8/PBAD, the Joint Staff Gatekeeper assigns POCs, as required, to participate in the FCB review.

3.4.2.3. Send the documentation to the Lead FCB via KM/DS. The Lead FCB will review the documentation, ensure the brief contains appropriate content, and schedule the follow-on activities (FCB WGs, FCB, JCB, JROC, etc.) through the KM/DS calendar function.

3.4.2.4. After the briefing cycle is completed, ensure the final briefing, appropriated notes, minutes and any associated JROCMs are attached to the record and archived in KM/DS.

3.4.2.5. For MDAPs, forward the appropriate JROCM, or like independent validation authority memorandum, to the MDA in support of SECDEF's Investment Review Process. The appropriate JROCM, or like independent validation authority memorandum, should include as a minimum the recommendations for program costs and fielding targets IAW Reference [13].

3.4.3. Updates to Sponsor validated capability requirements documents.

3.4.3.1. For changes to validated ICDs, IS-ICDs, CDDs, or IS-CDDs.

3.4.3.1.1. Following Sponsor approval of the change IAW References [17], [20], [22], [23], [24], [25], and [30], the Sponsor submits the updated document to the Joint Staff Gatekeeper with insight into any changes made to support FCB capability requirements portfolio management.

3.4.3.1.2. A description of the changes, rationale for the changes, and the revised document and its updated DoD Component validation memorandum will be posted in KM/DS and archived for future reference.

3.4.3.2. For changes to DoD Component UONs: Within 14 days of Sponsor approval of the change, the Sponsor submits the updated and validated DoD Component UON to the Joint Staff Gatekeeper for archiving.

3.4.4. Updates to JCB and JROC validated capability requirements documents based on Sponsor requests for changes to previous validation.

3.4.4.1. For significant changes to validated ICDs, IS-ICDs, CDDs, or IS-CDDs.

3.4.4.1.1. The Sponsor submits the updated document to the Joint Staff Gatekeeper for assessment in the required format at the time of submission.

3.4.4.1.2. The Joint Staff Gatekeeper assigns POCs from J-8/JCD, J-8 CAD, and J-8/PBAD, as required, to participate in the FCB review.

3.4.4.1.3. The Joint Staff Gatekeeper forwards the revised document to the appropriate lead FCBs and certification/endorsement authorities for review.

3.4.4.1.4. The Lead FCB and assigned AOs will evaluate the change and determine if staffing is required. JPR designation will be key in determining the level of staffing. Only those requirements designated as JPRs or sections of the document that have joint equity will be reviewed and assessed.

3.4.4.1.5. If additional staffing is required, the change will go through the normal staffing process based on its latest JSD and any associated JPRs.

3.4.4.1.6. If the Lead FCB Chair determines the revision affects one or more certifications or endorsements per Figure A-16, staffing is conducted through the appropriate stakeholders and certification or endorsement authorities to secure updated certifications or endorsements.

3.4.4.1.7. If additional staffing is not required, the Lead FCB will work with the Sponsor to prepare a briefing for the JROC/JCB to obtain approval.

3.4.4.1.8. The Lead FCB will schedule the briefing on the JCB and JROC calendars as required.

3.4.4.1.9. A revised validation memorandum is returned to the Sponsor once the revalidation is complete or the original validation reconfirmed.

3.4.4.2. For changes to validated JUONs or JEONs.

3.4.4.2.1. The Sponsor submits the updated document to the Joint Staff Gatekeeper, consistent with the classification level of the JUON or JEON and the guidelines outlined earlier in this enclosure.

3.4.4.2.2. The Joint Staff Gatekeeper forwards the updated document to the Lead FCB and JRAC for review.

3.4.4.2.3. The Lead FCB and JRAC will evaluate the change and determine if revalidation is required and will submit their recommendation to the validation authority.

3.4.4.2.4. If revalidated, the validation authority will send the Sponsor the revised validation memorandum.

3.5. Provide Common Gatekeeping with the:

3.5.1. IC Common Gatekeeper. IAW Reference [31], the IC maintains a common Gatekeeper function with the Joint Staff Gatekeeper for the ICCR and JCIDS processes. Capability requirements documents for both processes are submitted to the Gatekeeper to initiate staffing and ensure appropriate visibility and participation across processes.

3.5.2. DBS Common Gatekeeper. In support of Reference [32], the Office of the Chief Management Officer (OCMO) operates under a common Gatekeeper function with the Joint Staff Gatekeeper for the JCIDS process and for business systems requirements and acquisition where warfighter equity exists. DBS capability documents are submitted to the Joint Staff Gatekeeper to initiate staffing and ensure appropriate visibility and participation across processes.

3.5.3. Sponsor Organizations Gatekeepers. Sponsors organizations submitting and/or commenting upon capability requirements documents will have a Sponsor Gatekeeper function providing a single point of entry into the JCIDS process. Sponsor Gatekeeper(s) will facilitate communications between the Joint Staff Gatekeeper and principals in Sponsor organizations.

3.6. Manage the KM/DS system.

3.6.1. The Joint Staff Gatekeeper manages the organization of requirements data on the KM/DS system for data classified at or below the level of SECRET, and via other means for data classified above SECRET, and ensures that Sponsors provided studies or other data supporting their capability requirements documents prior to initiation of staffing. All metrics will be readily available on Knowledge Management and Decision Support site.

3.6.2. Stakeholders are notified of new capability requirements documents or data that are applicable to their respective capability requirements portfolios.

3.6.3. Any waivers to process and/or document formats are documented and archived with the associated documents for future reference.

3.7. Generate JCIDS Process Metrics. Process metrics tracked for JCIDS are outlined in Appendix D to this enclosure.

3.8. Manage submissions with special protections. Joint Staff Gatekeeper coordinates with the J-8/SAPCOORD and with the Sponsor to ensure that appropriately cleared stakeholders have access to capability requirements documents or issues protected by SAP, SAR, or ACCM designation.

3.8.1. Access will include the FCB Chair, and appropriate AOs from the FCB, J-8/JCD, J-8/PBAD, J-8/CAD, and certifying or endorsing organizations as needed to complete the review.

3.8.2. This ensures that decisions made regarding new capability requirements, and changes to validated capability requirements are considered in the context of the entire capability requirements portfolio.

APPENDIX D TO ENCLOSURE A
JCIDS STAFFING METRICS

1. Overview.

1.1. Purpose. The Joint Staff Gatekeeper generates metrics related to the JCIDS Processes and posts to the KM/DS system for visibility and potential process improvement action. To the maximum extent practical, metrics are intended to be automated from data available within the KM/DS system.

1.2. Applicability: These metrics apply to all documents within KM/DS.

1.3. Proponent: The proponent for this appendix is J-8/JCD. For questions, contact J-8/JCD at (703) 695-2705.

2. JCIDS Gatekeeping Metrics.

2.1. Timeliness Metrics.

2.1.1. Gatekeeper Time. Elapsed time from Sponsor document submission to the Joint Staff Gatekeeper assignment for staffing. Measure of Joint Staff Gatekeeper compliance with staffing timelines.

2.2. Performance Metrics.

2.2.1. Percent Accepted. Percent of documents initially accepted/rejected by the Joint Staff Gatekeeper. Measure of Sponsor submitted document quality.

2.2.2. Study Initiation Compliance. Percent of documents, based on CBAs or other studies, that Sponsors posted a study initiation notice prior to study initiation and study results prior to submitting document to the KM/DS study repository. Measure of Sponsor compliance with policy to reduce redundant studies, facilitate collaboration, and leverage historical studies.

3. JCIDS Deliberate Validation Metrics.

3.1. Timeliness Metrics.

3.1.1. Overall Time. Elapsed time from Sponsor document submission to signed JROCM. Measure of overall staffing time.

3.1.2. FCB WG Time. Elapsed time for FCB WG review. Measure of FCB WG compliance with staffing timelines.

3.1.3. Sponsor Time. Elapsed time for Sponsor comment adjudication. Measure of Sponsor compliance with staffing timelines.

3.1.4. FCB Chair Time. Elapsed time for FCB Chair Review and validation recommendation. Measure of FCB compliance with staffing timelines.

3.1.5. JCB Time. Elapsed time from FCB validation recommendation to validation by JCB. Measure of JCB compliance with staffing timelines.

3.1.6. JROC Time. Elapsed time from JCB validation recommendation to validation by JROC. Measure of JROC compliance with staffing timelines.

3.1.7. JROCM Time. Elapsed time from validation authority decision to signed JROCM being available in the KM/DS system. Measure of contribution to overall staffing time.

3.2. Performance Metrics.

3.2.1. Percent FCB Validation. Percent of documents receiving positive/negative FCB validation recommendations. Indirect measure of quality of Sponsor comment adjudication and/or indirect measure of significance of Sponsor proposed capability requirements to the capability requirements portfolio.

3.2.2. Percent Validation. Percent of documents validated/non-validated by validation authority. Indirect measure of FCB and validation authority alignment on intended direction for capability requirements portfolios.

4. JCIDS Urgent/Emergent Staffing Metrics. Note that the Joint Staff Gatekeeper maintains metrics on JUONs and JEONs. Generation of metrics for DoD Component UONs are at the discretion of the DoD Components.

4.1. Timeliness Metrics.

4.1.1. FCB/JRAC Time. Elapsed time for FCB WG and JRAC review. Measure of FCB WG and JRAC compliance with staffing timelines.

4.1.2. Validation Time. Elapsed time from FCB/JRAC recommendation to validation by the validation authority. Measure of validation authority compliance with staffing timelines.

4.2. Performance Metrics.

4.2.1. Percent FCB Validation. Percent of JUONs and JEONs receiving positive or negative FCB/JRAC recommendations. Indirect measure of significance of proposed capability to the capability requirements portfolio.

4.2.2. Percent Validation. Percent of JUONs and JEONs validated/non-validated by the validation authority. Indirect measure of FCB and validation authority alignment on direction for capability requirements portfolios and/or indirect measure of significance of Sponsor proposed capability requirements to the capability requirements portfolio.

5. JCIDS Post Validation Metrics.

5.1. Timeliness Metrics.

5.1.1. Time to Next Phase. Elapsed time from document validation to submission of successor document or fielding of capability solution(s). Measure of acquisition contribution to elapsed time.

5.1.2. Urgent/Emergent Transition Timeline. For JUONs and JEONs with assessments proposing enduring capability requirements, elapsed time from

assessment to submission of ICD for validation of enduring capability requirements.

5.2. Performance Metrics.

5.2.1. Tripwire Review Percent. Percentage of validated documents returning for revalidation due to JROC/JCB Tripwire review. Measure of Sponsor ability to meet validated capability requirements as proposed.

5.2.2. Nunn-McCurdy Percent. Percentage of validated documents returning for revalidation due to JROC/JCB Nunn-McCurdy breach review. Measure of Sponsor ability to meet validated capability requirements as proposed.

5.2.3. Percent Requirement Change. Percentage of validated documents returning for revalidation due to Sponsor proposed changes to requirements. Measure of requirement stability.

5.2.4. Urgent/Emergent Fielding Assessment. For JUONs and JEONs, elapsed time from fielded solution to CCMD submission of an assessment of operational utility of the fielded capability solution. Measure of CCMD compliance with policy to facilitate feedback and facilitate assessment of merits (or lack thereof) of validation as enduring capability requirements.

5.2.5. Urgent/Emergent Results. For JUONs and JEONs, percent of rapidly fielded capability solutions receiving each of the assessment categories – success/enduring requirement, success/limited sustainment, or failed/develop alternate capability solution.

5.2.6. Component UONs. For DoD Component UONs, number of DoD Component UONs submitted to the Joint Staff Gatekeeper for visibility.

(INTENTIONALLY BLANK)

ENCLOSURE B

JCIDS DOCUMENT FORMATS

1. Overview.

1.1. Purpose. The purpose of this enclosure is to provide Sponsors with a format guide for all JCIDS documents including the ICD, IS-ICD, CDD, IS-CDD, Joint DCR, and JUON/JEON.

1.2. Applicability. This enclosure applies to the Joint Staff, Services, CCMDs, and other DoD Agencies in situations as defined in the individual appendices.

1.3. Proponent. The proponent for this enclosure and all subordinate appendices is J-8/JCD. For questions, contact J-8/JCD at (703) 695-2705.

2. Formatting Standards.

2.1. General Document Formats.

2.1.1. Software compatibility. Latest available version of Microsoft Office.

2.1.2. Paper size and margins. Use 8.5-inch by 11-inch pages with 1-inch margins on all sides.

2.1.3. Font. For document content, use Times New Roman or Bookman Old Style 12-point. For classification (header and footer) markings, use Arial 24-point bold. Table content, use Arial or Calibri 10-point.

2.1.4. Style. Underline paragraph headings. Use bold only for emphasis within text. Use sentence case throughout text and uppercase for titles.

2.1.5. Spacing/alignment. Single-space draft and final versions. Double-space between paragraphs, bullets, and between titles and text. Left align text. Center titles.

2.1.6. Indentation. If formatted alpha-numerically, indent paragraphs 0.5 inch from the left margin. Indent subparagraphs an additional 0.5 inch from left margin. If formatted using scientific notation, indentation is optional.

2.1.7. Page numbering. For ease of identifying sections and page counts, the first page of the body of the document should start as page one. Front materials should be indexed with small Roman numerals, and appendices and/or annexes should start with A-1, B-1, C-1, and if used, D-1.

2.1.8. Line Numbering. To support review and staffing, documents will include line numbering.

2.2. Classification and Releasability.

2.2.1. All documents containing classified information will display appropriate classification and releasability markings (overall and portion) IAW Reference [33]. See Appendix C to Enclosure A of this manual for impacts of

classification on procedures for document submission to the Joint Staff Gatekeeper.

2.2.2. Sponsors will consider a foreign disclosure review when developing capability requirements documents that advocate for a future international acquisition program with allies and partner nations.

2.2.3. Capability requirements documents and supporting data are joint information, the release of which is governed by Reference [34]. See Reference [1] for additional responsibilities related to release of capability requirements documents and other JROC-related information.

APPENDIX A TO ENCLOSURE B
ICD

1. Overview.

1.1. Purpose. The purpose of an ICD is to document joint military capability requirements and associated capability gaps in cases where the Sponsor deems the operational risk of unmitigated capability gaps to be unacceptable.

1.1.1. The ICD provides traceability to the operational context, threats, and other relevant factors that determine the joint military capability requirements.

1.1.2. The ICD quantifies capability gaps associated with the requirements, operational risks across the joint force, and proposes materiel and/or non-materiel approaches to closing or mitigating some or all of the identified capability gaps.

1.2. Applicability. This appendix applies to the Joint Staff, Services, CCMDs, and other DoD Agencies.

1.2.1. For joint military capability requirements with a JSD of JROC or JCB Interest, Sponsors must strictly follow the format specified in this appendix, unless the Joint Staff Gatekeeper has granted a waiver in writing.

1.2.2. For service specific military capability requirements with a JSD of Joint Information, Sponsors should follow the format specified in this appendix. For consistency across documents, Sponsors must adhere to the same format for the capability requirement and gap/overlap table as specified in Figure B-1 of this appendix.

1.3. Proponent. The proponent for this appendix is the J-8/JCD. For questions, contact J-8/JCD at (703) 695-2705.

2. Format.

2.1. Cover Page.

2.1.1. Classification.

2.1.2. Title, starting with the phrase “Initial Capabilities Document for…”

2.1.3. Sponsoring organization, and signature authority who authorized the submittal for review and validation. The Sponsor GO/FO must endorse new ICDs, and modifications to validated ICDs.

2.1.4. Date submitted by the sponsoring organization.

2.1.5. Primary and secondary POCs for the document Sponsor. Include name, title/rank, phone, and both NIPRNET and SIPRNET email addresses. POCs must have completed the appropriate level of RMCT IAW Enclosure D of this manual.

2.1.6. Proposed validation authority.

2.1.7. Proposed MDA.

2.1.8. Proposed JSD, see Enclosure A of this manual for detail of JSDs.

2.1.9. Document revision number.

2.2. Validation Page.

2.2.1. While a document is in draft, a placeholder page will be included with the statement, "This document (include revision numbering) has not yet been validated and shall not be considered to be an authoritative source for the content herein. This document may be considered authoritative only when this page is replaced by a signed validation memorandum."

2.2.2. Once validated by the appropriate requirement validation authority, the placeholder page will be replaced by the signed validation memorandum.

2.2.2.1. For documents with JSD of JROC Interest or JCB Interest, the placeholder page will be retained until the signed JROCM is inserted. Any Sponsor approvals are not authoritative with respect to the document validation prior to JROC or JCB validation, and then only to the degree the JROCM delegates follow on authority to the Sponsor.

2.2.2.2. For documents with JSD of Joint Information, the Sponsor signed memorandum (or equivalent document) is authoritative with respect to the document validation.

2.2.3. If revisions to a document are proposed after validation, the placeholder page will be reinserted ahead of the original validation memorandum, until the updated validation memorandum is inserted. The original validation memorandum and memoranda validating subsequent changes, if applicable, are retained as part of the authoritative document.

2.3. Waivers (if applicable). In cases where the Sponsor was granted a waiver for format or content, a copy of the signed waiver or reference to the Joint Staff Gatekeeper's KM/DS approval note shall be included in the document so that all stakeholders understand the divergence of the document from the JCIDS format. For waivers to format, the Sponsor will include a "crosswalk" of the format sections/content that stakeholders expect to see based on current JCIDS guidance, and where that content can be found in the waived document format. This additional content immediately follows the waiver and does not contribute to page count limits.

2.4. Executive Summary. An executive summary, not to exceed one page, shall follow the validation page and precede the body of the ICD.

2.5. Document Body. The body of the ICD will have four sections and will be no more than 10 pages long.

2.5.1. Section 1: Operational Context.

2.5.1.1. The purpose of this section is to provide operational context for the capability requirements identified in the ICD. This information explains how

the capability requirements contribute to the missions and activities of the joint force.

2.5.1.2. Describe the range of military operations being addressed and the traceability to relevant parts of Unified Command Plan (UCP)-assigned missions, OPLANs/CONPLANs, SSA Products, Service and Joint Concepts, CONOPS, and/or other relevant factors to the capability requirements identified in the ICD. If operations are required in, or after exposure to, CBRN environments (i.e., chemical, biological, radiological, contamination and/or initial nuclear effects, such as High Altitude Electromagnetic Pulse (HEMP)), discuss how and where it fits in the operational context.

2.5.1.3. Identify the timeframe under consideration for IOC and FOC based on input from supported/supporting CCMDs and the acquisition community. The timeframes presented must be consistent with the DoDAF CV-3 and any phasing of capability requirements proposed in Section 3 of the ICD.

2.5.1.4. Identify what measurable operational outcomes are required; what effects must be produced to achieve those outcomes; how they complement the integrated joint/multinational warfighting force; and what enabling capabilities are required to achieve the desired operational outcomes.

2.5.1.5. Ensure any key intelligence support required capabilities to enable the capability solution's operational activities are addressed in this section.

2.5.1.6. Include the DoDAF OV-1 in this section, and where applicable, ensure high-level intelligence system connectivity and interoperability are accurately and adequately illustrated in the DoDAF OV-1.

2.5.1.6.1. Narrative in the operational context section must be consistent with the DoDAF OVs generated during prior analysis, as modified for the scope and purpose of the ICD, including the DoDAF OV-1, OV-2, OV-4, and OV-5a.

2.5.1.6.2. Do not include other architecture data and associated artifacts/views in the document unless specifically needed for illustration purposes.

2.5.2. Section 2: Threat Summary (Reference the Intelligence Supportability Guide described in Annex G to Appendix G of this enclosure)

2.5.2.1. The purpose of this section is to ensure that capability requirements and the associated capability gaps are based on consistent threat environment information and references. Sponsors must provide traceability to the most current DIA- or Service-approved threat products used to support their ICD.

2.5.2.2. Cite the threat products used during the development of the capability requirements identified in the ICD.

2.5.2.3. Identify all anticipated capabilities that adversaries might employ against the capability being reviewed and provide sufficient information and analysis to support DIA/TLA's threat assessment. This information and analysis should address capability requirements and associated capability gaps

related to the conduct of operational tasks and missions, rather than only defining threats to a future capability solution and their associated performance parameters.

2.5.2.4. Provide a description of all threat capabilities, threat tactics, and adversary doctrine, if available, in the expected operational environment and the nature of current and anticipated threats which are a factor in setting the capability requirements and initial objective values. Include any CBRN, space, cyber, or kinetic threats and/or threats to a future system's use of the electromagnetic spectrum if the operational context requires operation in such environments.

2.5.2.4.1. Ensure judgments or extrapolations regarding adversarial capabilities are appropriate, logical, complete, and consistent with DIA- and Service-approved threat products.

2.5.2.4.2. Consider threats to follow-on research, development, testing and evaluation (RDT&E), production, and operation and maintenance (O&M) resulting from technology transfer, espionage, and other adversarial collection efforts.

2.5.2.4.3. Consider threats that are likely to evolve or change to ensure flexibility in capability requirements.

2.5.2.4.4. Threats are factors that an adversary can control and direct, or will be able to direct, and do not include environmental or natural factors such as weather or terrain.

2.5.2.5. Cite any related CIPs, either as approved CIPs or as proposed new CIPs for review and approval in conjunction with ICD validation.

2.5.2.5.1. CIPs will be included for capabilities in development that are determined to be threat-sensitive.

2.5.2.5.2. Sponsors should coordinate with DIA during the development of the requirement to determine whether the capability is threat-sensitive and/or if a CIP(s) is required.

2.5.2.5.3. CIPs (IAW Reference [35]) are defined as a threat capability or threshold established collaboratively by the requirements sponsor and the capability developer, changes to which could critically impact the effectiveness and survivability of the proposed system.

2.5.3. Section 3: Capability Requirements and Gaps/Overlaps.

2.5.3.1. The purpose of this section is to specify capability requirements and to assess associated capability gaps in terms of a comparison between the capability requirement and current capability solutions available to the joint force or in development.

2.5.3.2. In separate paragraphs, define capability requirements in the following manner: "The ability to [perform a task (UJT or Service Task) Operational

Activity]] against/given a [Threat] in order to achieve [Effect] in a/under [Environmental Conditions] in the [Standard Timeframe]." Capability requirements must be general enough so as not to create the appearance of a predetermined capability solution or solution approach (e.g., new system, FoS, SoS) but specific enough to evaluate alternative means to achieve the capability.

2.5.3.2.1. Operational Activity. This is what the capability must do or perform to satisfy one or more tasks. Although not limited to, the operational activities should be described in the lexicon of the Universal Joint Tasks (UJTs) or DoD Component equivalents.

2.5.3.2.2. Threat. Detailed threat analysis is critical for friendly force mission planning and defense suppression across all domains. The Joint Intelligence Preparation of the Operational Environment (JIPOE) alerts decision-makers at all echelons to potential emerging situations and threats. The threat that a capability is designed to neutralize or defeat to successfully complete a specified mission must be clearly identified. The threat should be consistent with the JIPOE conducted for the joint commander.

2.5.3.2.3. Effect. The operational effect or end state that is required for the capability to achieve that will enable the successful completion of the mission in support of the NMS.

2.5.3.2.4. Physical Areas and Factors: The environmental and other non-threat related conditions in which the capability must operate are also identified. These conditions should be consistent with those found in the JIPOE.

2.5.3.2.5. Timeframe. The expected timeframe the capability needs to be available for, must be consistent with the IOC and FOC timelines in the ICD.

2.5.3.2.6. Example. "The ability to collect operational information given an advanced A2/AD threat environment in order to maintain situational awareness of enemy movements in an urban environment in the 2030 timeframe."

2.5.3.3. For each capability requirement, specify the required operational attributes with appropriate quantitative parameters and metrics, e.g., outcomes, time, distance, effect (including scale), obstacles to be overcome, supportability, etc. See Annex A to Appendix B of Enclosure C to the manual for examples of operational attributes.

2.5.3.3.1. Indicate the initial objective value for each operational attribute to provide a discrete value that satisfies the operational need(s) for the capability. This will serve as the starting point for analysis supporting capability requirement trade-offs above and below the initial objective value. In the narrative portion of the requirement, describe the operational implications that drive the value to be proposed at the specified level. Consider the effects of cybersecurity and any required additional support needed from the IC in

determining the initial objective values, as described in paragraphs 2.5.3.4. and 2.5.3.5. below.

2.5.3.3.1.1. Initial objective values are the values necessary to achieve mission objectives with moderate operational risk. The narrative should explain why the capability requirements are essential to the Sponsor in order to achieve assigned goals and objectives. Include assessment of operational implications - increased or decreased operational risks - which may be a factor as capability requirements are traded up or down during follow-on analysis and development efforts.

2.5.3.3.1.2. Values listed as "TBD," those specified only as a ratio relative to the value of a legacy capability solution, or operational attributes without quantifiable measures, are not allowed. In such cases, the Sponsor is not ready to document capability requirements in an ICD and must perform additional analysis based on the applicable Service and Joint Concepts or CONOPS before finalizing the ICD.

2.5.3.3.2. The narrative, attributes, and values in the capability requirement and capability gap section must be consistent with DoDAF CVs generated during prior analysis, as modified for the scope and purpose of the ICD, including the DoDAF CV-2, CV-3, and CV-6.

2.5.3.4. Intelligence supportability to the capability requirements. If known, Sponsors should include in the narrative portion of the requirement a description of the intelligence support requirements and resources needed to enable each capability requirement. This description will be provided by identifying the intelligence support categories applicable to each capability requirement and identifying the support requirements and resources within each category. Sponsors should refer to Annex G of Appendix G to this enclosure for a definition of the intelligence support categories.

2.5.3.5. System Survivability Considerations.

2.5.3.5.1. Cybersecurity/ Cyber Survivability Considerations. Capability requirements should also consider the cybersecurity threat when determining initial objective values and include an exemplar statement(s) in the ICD for the appropriate Cyber Survivability Risk Category (CSRC). This exemplar statement can be provided in Section 3 of the ICD (either in the narrative or as part of the Capability Requirements and Gap/Overlap Table) or it can be provided as Appendix E to the ICD. Refer to Annex C to Appendix G of this enclosure and the Cyber Survivability Endorsement Implementation Guide which can be found on KM/DS IAW Reference [4] for more details. In addition, the ICD should identify the system categorization for information systems and Platform IT (PIT) systems as a required capability - the potential impact (low, moderate, or high) resulting from loss of confidentiality, integrity, and availability if a security breach occurs. This is required by DoD's Risk Management Framework for Information Technology Systems (Reference [12]

2.5.3.5.2. EMS Survivability Considerations. Capability requirements should also consider EMS threats when determining initial objective values and include exemplar statement in the ICD for the appropriate EMS Survivability Risk Category. This exemplar statement can be provided in Section 3 of the ICD (either in the narrative or as part of the Capability Requirements and Gap/Overlap Table) or it can be provided as Appendix F to the ICD. Refer to Annex C to Appendix G of this enclosure and the DoD Guidebook for Electromagnetic Spectrum Survivability which can be found on KM/DS IAW Reference [4] for EMS Survivability requirements.

2.5.3.6. In a new paragraph for each requirement, describe the capability gaps or overlaps in terms of the difference between the initial objective values and the performance levels of capability solutions currently available to the joint force or in development. Identify those capability requirements for which there exist overlaps or redundancies, including considerations of existing or planned capabilities in other DoD Components; U.S. Government agencies or departments; and allied or partner nations. Assess whether the overlap is advisable for operational redundancy or if the overlap is a potential tradeoff to satisfy other identified capability gaps.

2.5.3.6.1. When describing “current capabilities” in the narrative paragraphs, Sponsors must consider all PORs and rapidly fielded capability solutions in the joint force. This should be consistent with the market research conducted as part of the CBA described in Annex B to Appendix B to Enclosure C of this manual.

2.5.3.6.1.1. Sponsors may not exclude viable capability solutions from the comparison because they are not the Sponsor’s preferred solution, or because they are developed and operated by another DoD Component.

2.5.3.6.1.2. Sponsors must ensure review of identified capability gaps by someone with visibility into capability solutions protected by higher classification levels.

2.5.3.6.1.3. If identified capability gaps would be different in light of capability solutions protected by higher classification levels, Sponsors may provide supplemental data in the form of a classified appendix as described at the end of the ICD format guidance.

2.5.3.6.2. When describing a recapitalization (or “next generation”) situation, the “current capabilities” must consider the capability solution being replaced, as well as other viable solutions as noted above. Life extension or continuing/restarting production of the fielded capability solution, or possibly leveraging portions of fielded capability solutions, may be part of tradeoff discussions and/or follow-on AoA activities.

2.5.3.7. Clearly identify how each capability gap identified impacts the operational context in Section 1 of the ICD, in terms of inability to execute part or all of an operational plan and/or unacceptable levels of operational risk. Where workarounds are feasible until the requirements proposed in the ICD

are satisfied by capability solutions, then identify the workarounds and operational risk(s) associated with them.

2.5.3.8. Summary table. Provide a summary table for the relationship between capability requirements in each JCA (Tier 2) and relevant operational attributes and associated gaps/overlaps with respect to current or programmed force capabilities in a table as shown in Figure B-1. Sponsors should relate capability requirements to the lowest tier possible.

Capability Requirements			Current Capabilities		Significant Gap(s)/Overlap(s)
	Operational Attribute[1]/Metric	Initial Objective Value	Source/ System	Current Performance	
1. Capability Requirement			JCA 2.2: BA/Collection		Briefly describe the most significant gap(s) and or overlap(s) for the requirement.
	Attribute 1.1	Value (no TBDs)	System 1	Value (no TBDs)	
			System n	Value (no TBDs)	
	Attribute 1.n	Value (no TBDs)	System 1	Value (no TBDs)	
			System n	Value (no TBDs)	
2. Capability Requirement			JCA 3.1: FA/Maneuver		Sponsors should limit this to one sentence; preferably less than 15 words.
	Attribute 2.1	Value (no TBDs)	System 1	Value (no TBDs)	
			System n	Value (no TBDs)	
	Attribute 2.n	Value (no TBDs)	System 1	Value (no TBDs)	
			System n	Value (no TBDs)	
n. Capability Requirement			JCA X.x: Tier 1/Tier 2		See above
	Attribute N.1	Value (no TBDs)	System 1	Value (no TBDs)	
			System n	Value (no TBDs)	
	Attribute N.n	Value (no TBDs)	System 1	Value (no TBDs)	
			System n	Value (no TBDs)	
			System n	Value (no TBDs)	

Note:
[1] Attribute information is located in Annex A to Appendix B to Enclosure C beginning on Page C-B-A-1.

Figure B- 1: Capability Requirements and Gap/Overlap Table

2.5.3.8.1. In cases where phased introduction of capabilities is appropriate to the Joint or Service concepts or CONOPS, different levels of capability requirements can be listed for different timeframes and must be consistent with the DoDAF CV-3.

2.5.3.8.2. This table will serve as a guide for development of follow-on JCIDS documents.

2.5.3.8.3. TBD values are not allowed for either the initial objective value or the current performance. The Joint Staff Gatekeeper will reject documents with TBD in these sections.

2.5.4. Section 4: Final Recommendations.

2.5.4.1. The purpose of this section is to identify one or more paths forward to satisfy the capability requirements and close or mitigate associated capability gaps identified in the document. Ensure recommendations reflect a thorough understanding of the threat considerations, intelligence support requirements, and capabilities for the functional and operational areas.

2.5.4.2. Identify DOTmLPF-P recommendations to be considered as part of a materiel solution and independent of a materiel solution.

2.5.4.3. Specify the preferred type of materiel approach, if the requirement cannot be met using non-materiel approaches, to eliminate or mitigate each capability gap. This information may be used by the MDA to inform the scope of the AoA or similar study. Approaches include:

2.5.4.3.1. Evolution of a fielded capability solution(s) with significant capability improvement, including development and fielding of improved IS, improved components or subsystems to address high obsolescence rates, or other upgrades and product improvements.

2.5.4.3.2. Replacement or recapitalization of a fielded capability solution(s) with significant capability improvement. The ICD will describe plans to retire fielded capability solution(s) as the new capability solution(s) is brought into service and whether quantities in the joint force should be reduced based on increases in capability.

2.5.4.3.3. Introduction of a transformational capability solution(s) that differ significantly in form, function, and/or operation from fielded capability solution(s). This may address gaps associated with a new mission, describe breakout capability solution(s) that offer significant improvement in capability, or transform the ways of accomplishing a mission.

2.5.4.3.4. Evolve and combine existing and new systems to create synergistic SoS. Examples include creating joint integrated kill chains for air and missile defense or integrated SoS for creating layered defense designs.

2.5.4.3.5. Leverage S&T to reduce operational risk(s), ensuring technologies are sufficiently mature prior to initiation of a new or enhanced capability solution. Identify ongoing or new developmental technologies that have the potential to eliminate or mitigate capability gaps. Emphasize technologies that enhance joint warfighting capability against emerging threats and/or increase affordability within the capability requirements portfolio.

2.5.4.4. Acceptance of operational risk. Not every identified capability gap needs to be immediately addressed by a capability solution or S&T effort. A relatively low priority of the capability requirement to the overall joint force may not justify the lifecycle costs of taking further action at the present time.

2.5.4.5. Affordability. When writing an ICD, the Sponsor should not have a predetermined capability solution in mind, nor the level of required detail to produce associated cost estimates. Additionally, multiple services may develop capabilities based on a different sponsor's ICD and the initial Sponsor may not have insight into these development efforts. However, a constrained fiscal environment with competing demands for resources requires that Sponsors consider affordability in the development of an ICD.

2.5.4.5.1. The ICD should identify key factors that the Sponsor knows of, that may be, or may become, significant cost drivers for potential materiel solutions

that may flow from the ICD. This information can help DoD focus S&T and risk reduction efforts, thereby potentially reducing the resources needed to satisfy joint military capability requirements and eliminate or mitigate the associated gaps identified in the ICD.

2.5.4.5.2. This information will inform lifecycle cost, performance, schedule, and quantity tradeoff discussions in follow-on efforts, such as in the AoA, and subsequent requirements and acquisition decision making.

2.5.4.5.3. Since ICDs should be solution agnostic, there may be multiple AoAs and multiple programs associated with a single ICD, making an accurate cost estimate extremely difficult at this point in the development process. Once information is further developed or known, it may be necessary to perform a revised cost-estimate.

2.6. Appendices. The following appendices are allowed in the document.

2.6.1. Appendix A. References. Ahead of other references provided in this appendix, provide an accessible URL for required architecture data and associated artifacts/views identified in Figure A-4 and, if applicable, Figure B-20. The URL location must be discoverable and accessible IAW Appendix H to Enclosure B of this manual.

2.6.2. Appendix B. Acronym List. List in alphabetical order, all of the acronyms used in the document.

2.6.3. Appendix C. Glossary. As the Sponsor develops the document glossary, they may leverage applicable definitions from the DoDAF AV-2. These do not have to be identical as some terms will apply only to the document or the DoDAF architecture; however, terms that apply to both must be consistent.

2.6.4. Appendix D. (Optional) Classified Appendix. A classified appendix may be used in cases where only a small subset of the document needs to be protected at a higher classification level. If the document is not useful without this appendix, the document is to be classified at a higher level. A classified appendix's content will count toward the document body page limits and will be indexed to align with the baseline document sections. Except where the existence of classified content cannot be acknowledged, each section of the baseline document augmented by the classified appendix will refer the reader to the classified appendix. If used, the appendix shall be provided to the Joint Staff Gatekeeper or J-8/SAPCOORD IAW the classification of the appendix.

2.6.5. Appendix E. Cyber Survivability Risk Categories (CSRC). Sponsor will use this appendix to determine the CSRC of the capability requirement and describe Cyber Survivability Attribute requirements IAW Annex C to Appendix G of this enclosure and the Cyber Survivability Endorsement Implementation Guide which can be found on KM/DS, Reference [4].

2.6.6. Appendix F. EMS Survivability Risk Category. Sponsor will use this appendix to determine the EMS Survivability Risk Category and describe it IAW

Annex C to Appendix G of this enclosure and the EMS Survivability Guidebook which can be found on KM/DS, Reference [4].

APPENDIX B TO ENCLOSURE B

IS-ICD

1. Overview. The IS-ICD is a variant of the regular ICD, implementing the "IT Box" construct outlined in this section. IS-ICDs streamline the requirements process by delegating oversight and formats for subsequent documents as identified in the IS-ICD. This provides IS programs greater flexibility to incorporate evolving technologies and achieve faster acquisition.

1.1. Purpose. The purpose of an IS-ICD is to facilitate efficient and timely software development efforts; IS-ICDs are not appropriate for hardware development efforts or capturing capability requirements that span a broad scope of hardware, software, and/or DOTmLPF-P efforts. The IS-ICD serves as the basis for validation by the validation authority identified in Enclosure A of this manual. Any streamlining of acquisition processes is at the discretion of the MDA IAW References [5] and [9].

1.2. Applicability.

1.2.1. IS-ICDs are appropriate for:

1.2.1.1. When it is clear from the CBA that an IS solution is the only viable approach to be considered.

1.2.1.2. The procurement or modification of GOTS/COTS IS products is from domestic or international sources, or the development of dual-use technologies.

1.2.1.3. The additional production or modification of developed DoD, allied, partner-nation, or other U.S. Government agency IS products.

1.2.1.4. Development, integration, and acquisition of customized application software, including commercial IS capability solutions with integrated, DoD-specific performance characteristics/standards.

1.2.1.5. All hardware associated with an IS-ICD must be COTS/GOTS. Hardware modifications are restricted to those necessary for integration, enhancements to meet requirements specified in the IS-ICD, or hardware refresh due to obsolescence.

1.2.1.6. The development of both offensive and defensive cyber capability that meet the remaining criteria for an IS-ICD and require the flexibility that the IT process provides.

1.2.1.7. Approaches where the capability solution involves research, development, and/or acquisition of applications systems software, and the projected lifecycle costs exceed $15 million. IS-ICDs with lifecycle costs less than $15 million may be submitted for review and validation if validated requirements are needed to support budgetary requests or other purposes.

1.2.2. IS-ICDs are not appropriate for:

1.2.2.1. Software embedded in a capability solution developed under other validated capability requirements documents. In this case, the software requirements are validated as part of the overall capability solution.

1.2.2.2. Software requiring a host platform, such as a manned or unmanned vehicle, which does not yet have validated capability requirements documents. In this case, the software requirements can be included in the capability requirements of the host platform or as a separate IS-ICD.

1.2.2.3. Increases in quantities of fielded IS without modification, not developed by an "IT Box" should be addressed by a DCR.

1.2.2.4. Requirements for DBS capabilities defined and acquired IAW References [36] and [37].

1.2.3. In cases where the potential for use of the "IT Box" construct is unclear or in dispute, the Joint Staff Gatekeeper, in consultation with the validation authority as needed, will determine whether an ICD or IS-ICD will be used.

1.2.4. Joint command and control (C2) requirements that have a validated IS-ICD will be identified, documented, validated, prioritized, managed, and monitored IAW [11].

1.2.5. Annual/Biennial FCB Review of IS Systems. Annual/Biennial FCB Review for IS programs. For all IS programs with a valid IS-ICD, the Sponsor shall provide the Lead FCB an update a year following the validation and then biennially after. For an IS-CDD, the Sponsor shall provide the Lead FCB an update every second year following the validation. The Lead FCB will determine if the JROC or JCB should review the following items and will make appropriate recommendations for action.

1.2.5.1. Progress in delivering capability solutions within the required timeframe and available funding.

1.2.5.2. Compliance with applicable EA and data standards.

1.2.5.3. Other items as identified by the IS-ICD validation.

1.3. Proponent. The proponent for this appendix is the J-8/JCD. For questions, contact J-8/JCD at (703) 695-2705.

2. Format.

2.1. Cover Page. The cover page for an IS-ICD shall be the same as for a regular CDD except that the title will begin with the phrase "Information Systems Initial Capabilities Document for…"

2.2. Validation Page. No change from a regular ICD to the validation page for an IS-ICD.

2.3. Waivers (if applicable). No change from a regular ICD to the waiver section for an IS-ICD.

2.4. Executive Summary. No change from a regular ICD to the executive summary in the IS-ICD.

2.5. Document Body. The body of an IS-ICD differs from a regular ICD in two sections and shall be no more than 10 pages long including any content modified or augmented by a classified appendix, if used. See the regular ICD section for content of the unchanged sections.

2.5.1. Section 1: Operational Context. No change from a regular ICD to the operational context section in the IS-ICD.

2.5.2. Section 2: Threat Summary. No change from a regular ICD to the threat summary of the IS-ICD; however, the Sponsor should strongly consider the cyber threats posed to an IS solution.

2.5.3. Section 3: Capability Requirements and Gaps/Overlaps. Same as the regular ICD with the addition of the following:

2.5.3.1. Include a net-ready performance attribute table, reference Figure B-2 and describe each attribute in terms of initial minimum values rather than threshold and objective values.

NR Performance Attribute	Performance Parameter[1]	Initial Minimum Value
Support to Military Operations	**Mission:** *Security Qualitative Capability (SQC)[2] Mission is to plan, request, coordinate, and control Close Air Support (CAS) missions, and provide C2 situational awareness, in support of joint and coalition ground maneuver forces.*	
	Mission Activity: *Provide voice and data communications with mission partners.* **Measure:** *Accuracy of SQC information; consistently processed, stored, and made available to user or external consumer exactly as obtained.*	*≥ 99%*
	Mission Activity: *Provide situational awareness* **Measure:** *Accuracy of mission update messages from other C2 platforms.*	*≥ 99%*
	Conditions: *Adverse weather, day/night air transport operations in permissive to low threat environment.*	

NR Performance Attribute	Performance Parameter[1]	Initial Minimum Value
Enter and Manage in the Network	**Network**: *NIPRNET.* **Measure:** *Time to connect to an operational network from power up.*	*≤ 1 minute*
	Network: *SIPRNET.* **Measure:** *Time to connect to an operational network from power up.*	*≤ 5 minutes*
	Network: *Link-16.* **Measure:** *Time to connect to an operational network from power up.*	*≤ 2 minutes*
	Measure: *Availability of network during adverse weather conditions.* **Condition:** *Continuous Network Connectivity based on system-controllable factors.*	*≥ 99%*
Exchange Information	**Information Element:** *Support Data.* **Measure:** *Time to exchange data between SQC and System A (NGA).*	*≤ 2 minutes*
	Information Element: *Target Data.* **Measure:** *Time to exchange data between SQC and System B (NSA).*	*≤ 2 minutes*
	Information Element: *ISR Data.* **Measure:** *Time to exchange data between SQC and System C (USCENTCOM).* **Conditions:** *NSA Type 1 Certified Encryption Systems in operation and continuous network connectivity.*	*≤ 2 minutes*

Note:
[1] **Bold text is the template**; *non-bold and italicized text provides an example*.
[2] Security Qualitative Capability (SQC) is a fictitious program for the purposes of this template.

Figure B- 2: Net-Ready Performance Attribute IS-ICD Example

2.5.4. Section 4: Final Recommendations. Same as the regular ICD with the addition of the following:

2.5.4.1. Development of the "IT Box."

2.5.4.1.1. The "IT Box" construct, Figure B-3, calls for fewer iterations of validating capability requirements documents through the JCIDS process by describing the overall IS program and delegating validation of detailed follow-on requirement and solution oversight to a flag-level organization other than the JROC or JCB.

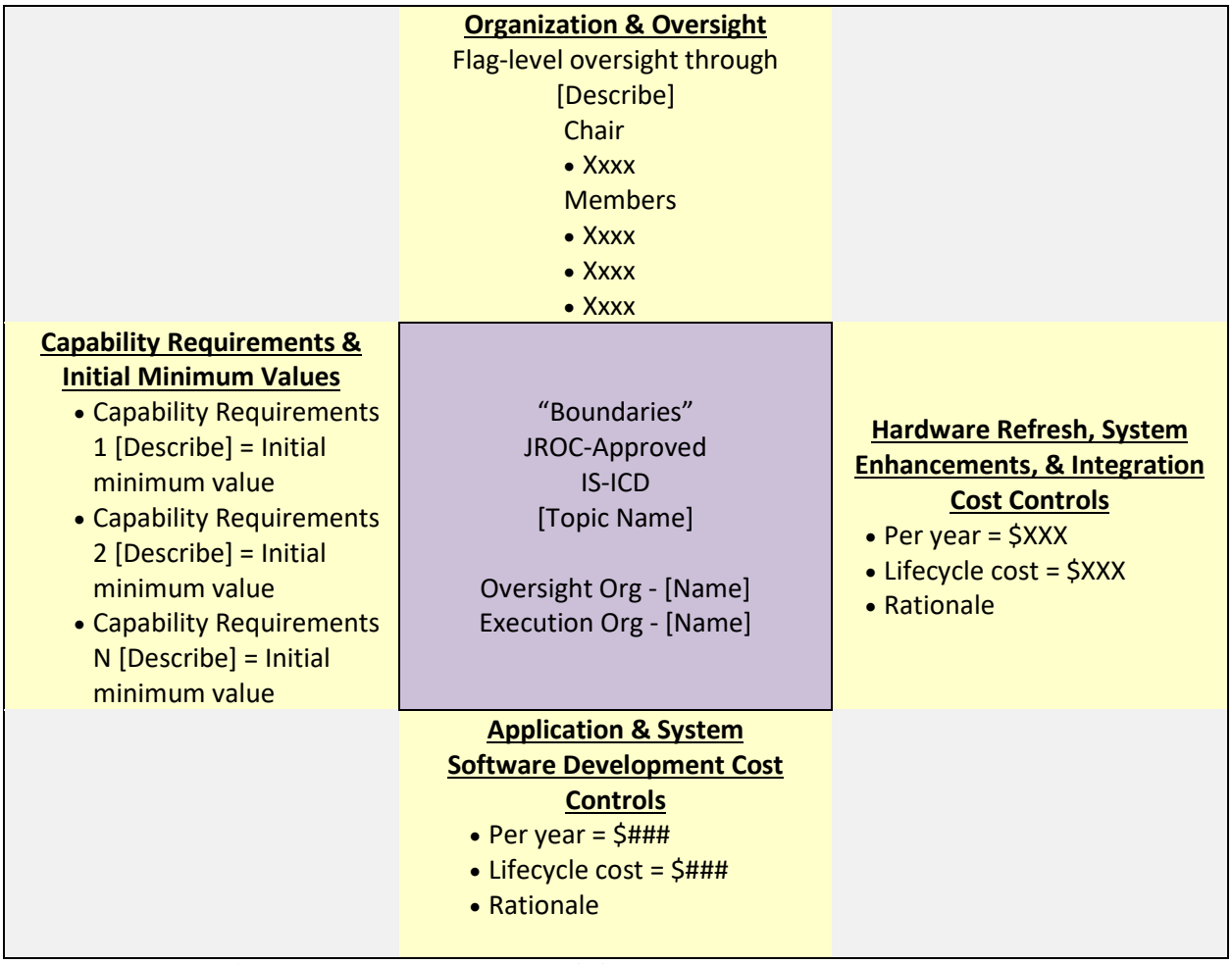

Figure B- 3: Components of the "IT Box" Construct in IS'ICDs

2.5.4.1.1.1. The "IT Box" model uses initial minimum values in place of initial objective values so that the baseline capability is clearly specified, and the delegated oversight body has flexibility to further develop capabilities without revalidation of the capability requirements document.

2.5.4.1.1.2. Initial minimum values represent the achievable level of required capability needed to incorporate current technology to meet the baseline capability.

2.5.4.1.1.3. Successor documents must be provided to the KM/DS system for information purposes and visibility in the capability requirements portfolios.

2.5.4.1.2. Inclusion of lifecycle costs for the program. Break out costs into annual estimates of development and integration as well as sustainment costs as shown in Figure B-4.

Required Resources:									
BY$$[2]	**FYxx (Current)**	**FYDP**						**Post-FYDP (FYyy-FYzz)**	**Life Cycle Cost (FYxx-FYzz)**
		FYxx+1	**FYxx+2**	**FYxx+3**	**FYxx+4**	**FYxx+5**	**FYDP Total**		
Application and System Software Development Costs									
RDT&E[3]									
Procurement[3]									
MILCON[3]									
O&M[3]									
MILPERS[3]									
Total									
Hardware Refresh, System Integration									
RDT&E[4]									
Procurement[4]									
MILCON[4]									
O&M[4]									
MILPERS[4]									
Total									
Overall Total									

Notes:
[1] Current year is FYxx. First post-FYDP year is FYyy. End of planned capability life, or end of 30-year TOA projection if no planned service life, is FYzz.
[2] All resources normalized to a standard base year reference - BY$$.
[3] Application and System Software Development Costs.
[4] Hardware Refresh, System Integration Costs.

Figure B- 4: Example Lifecycle Cost Summary Table for IS-ICDs

2.6. Appendices. The appendices for an IS-ICD are the same as for a regular ICD.

APPENDIX C TO ENCLOSURE B
CDD

1. Overview. The CDD provides traceability to predecessor documents and validated capability requirements, provides supporting data for certifications and endorsements, identifies related DOTmLPF-P impacts of the proposed capability solution, and outlines projected lifecycle costs that are expected to result from pursuing the capability solution.

1.1. Purpose. The purpose of a CDD is to propose development of a materiel capability solution intended to wholly or partially satisfy approved capability requirements in order to close or mitigate associated capability gaps for which the DoD does not want to accept operational risk.

1.1.1. The CDD provides performance attributes (KPPs, KSAs, and APAs) to guide the development and production of one or more increments of a system. Each increment described by a CDD must provide a safe, operationally effective, suitable, and useful capability solution in the intended environment, commensurate with the investment.

1.1.2. The original CDD, including the performance attributes and other related sections, may remain valid through production requiring no additional staffing or coordination, unless there is a significant change that would require an update to the original validated CDD. In this case, a CDD Update will be required and validated by the same validation authority of the original document. Deliberate staffing and review will be used for CDD Updates in the same manner as CDDs with the exception that the only sections for review and validation will be the updated sections of the document. Sponsors may request expedited staffing for CDD Updates. Reference the CDD Update section under Appendix A of Enclosure A of this manual for more information on the staffing of CDD Update documents.

1.1.3. The CDD serves as the basis for validation by the appropriate validation authority identified in Enclosure A of this manual.

1.2. Applicability. This appendix applies to the Joint Staff, Services, CCMDs, and other DoD Agencies.

1.3. Proponent. The proponent for this appendix is the J-8/JCD. For questions, contact J-8/JCD at (703) 695-2705.

2. Format.

2.1. Cover Page.

2.1.1. Classification.

2.1.2. Title, starting with the phrase “Capability Development Document for…”

2.1.3. Sponsoring organization and signature authority who authorized the submittal for review. The Sponsor GO/FO must endorse new CDDs and modifications to validated CDDs.

2.1.4. Date submitted by the Sponsoring organization.

2.1.5. Primary and secondary POCs for the document Sponsor. Include name, title/rank, phone, and both NIPRNET and SIPRNET email addresses. POCs must have completed the appropriate level of RMCT IAW Reference [1].

2.1.6. Proposed validation authority.

2.1.7. Proposed MDA.

2.1.8. Proposed JSD, see Enclosure A of this manual for detail of JSDs.

2.1.9. Proposed JPRs, see Enclosure A of this manual for detail of JPRs. (List the JPRs by referring to which KPPs identified IAW Figure B-6 are proposed to be JPRs. For example, if KPP #2 and #3 are considered to be JPRs, then you would state "JPRs: KPPs #2 and #3")

2.1.10. Proposed ACAT.

2.1.11. Document revision number.

2.2. Validation Page.

2.2.1. While in draft, a placeholder page will be included, with a statement of: "This document (include revision numbering) has not yet been validated and shall not be considered an authoritative source for the content herein. This document may be considered authoritative only when this page is replaced by a signed validation memorandum from the appropriate validation authority."

2.2.2. Once validated by the validation authority, the placeholder page will be replaced by the signed memorandum indicating validation of the document.

2.2.2.1. For documents with JSD of JROC or JCB Interest, the placeholder page will be retained until the signed JROCM is inserted. Any Sponsor approvals prior to JROC or JCB validation are not authoritative and do not replace the placeholder validation page.

2.2.2.2. For documents with JSD of Joint Information, the Sponsor-signed memorandum (or equivalent document/form) is authoritative with respect to the document validation.

2.2.3. If revisions to a document are proposed after validation, the placeholder page will be reinserted ahead of the original validation memorandum, until the updated validation memorandum is inserted. The original validation memorandum and subsequent revisions are retained as part of the authoritative document.

2.3. Waivers (if applicable). In cases where the Sponsor was granted a waiver for format, content, and/or page count, a copy of the signed waiver or reference to the Joint Staff Gatekeeper's KM/DS approval note shall be included in the

document so that all stakeholders can more easily understand the divergence from the standard JCIDS document. For waivers to format, the Sponsor will include a "crosswalk" of the format sections/content that stakeholders expect to see based on current JCIDS guidance, and where that content can be found in the waived document format. This additional content immediately follows the waiver and does not contribute to page count limits.

2.4. Executive Summary. An executive summary, not to exceed one page, will follow the validation page and precede the body of the CDD.

2.5. Document Body. The body of the CDD will have 13 sections and will be no more than 45 pages long.

2.5.1. Section 1: Operational Context.

2.5.1.1. The purpose of this section is to provide the operational context in which the capability requirements defined in the ICD are being addressed by the proposed CDD. This information explains how the capability solutions contribute to the missions and activities of the joint force.

2.5.1.1.1. The narrative in the operational context section is to be consistent with DoDAF OVs generated during prior analysis, as modified for the scope and purpose of the CDD, including the DoDAF OV-1, OV-2, OV-4, and OV-5a. In cases where these DoDAF OVs are not available for updating, they shall be generated to support the CDD.

2.5.1.1.2. Provide the DoDAF OV-1 in this section. If applicable, include intelligence system connectivity and interoperability in the DoDAF OV-1. Do not include any other DoDAF views in this section unless specifically referenced elsewhere in the body of the CDD.

2.5.1.2. Cite the validated source documents that identify the capability requirements addressed by the CDD and ensure that any source documents not already present in KM/DS are provided to the Joint Staff Gatekeeper for reference purposes.

2.5.1.3. From the source document(s), summarize the operational context(s) associated with the validated capability requirements addressed by the CDD. Ensure that any changes to operational context(s) that have occurred since validation of the capability requirements are addressed in this section. If any changes to the operational context have been made, ensure the DoDAF OVs submitted with the ICD are updated to reflect the changes.

2.5.1.4. Additionally, if the CDD is not based on a validated capability requirements document, provide the operational context and initial DoDAF OVs as outlined for Section 1 of an ICD.

2.5.2. Section 2: Threat Summary. (Reference the Intelligence Supportability Guide described in Annex G to Appendix G to this enclosure)

2.5.2.1. The purpose of this section is to ensure the capability solution(s) being developed to address the capability requirements and associated gaps are based on consistent threat environment information and references. All acquisition programs or capabilities expected to operate in a threat environment (lethal or non-lethal) must be developed IAW the most current DIA- or Service-approved threat products.

2.5.2.2. Cite the latest DIA- or Service-approved threat products used during the development of the CDD. Update the applicable threat information since validation of the ICD and clearly identify threats that were factors in determining the capability requirements captured in the ICD.

2.5.2.3. From the source document(s), outline the threat summary(ies) associated with the validated capability requirements addressed by the CDD. Consider evolving threats to on-going and follow-on RDT&E, production, and O&M resulting from technology transfer, espionage, and other adversarial collection efforts.

2.5.2.3.1. Summarize approved CIPs, in the manner expressed below, that are applicable to the KPPs in the CDD. These can be approved CIPs that are being monitored by the IC and/or proposed CIPs that are currently under review and approval in conjunction with the CDD validation.

2.5.2.3.1.1. Describe the relationship between the CIP and the supported KPP.

2.5.2.3.1.2. Cite the Community On-Line Intelligence System for End Users and Managers (COLISEUM) production requirement number, the Defense Acquisition Management Information Retrieval (DAMIR) long name and/or DAMIR short name, CIP number, and threat topic.

2.5.2.3.1.3. CIPs (IAW Reference [35]) are defined as a threat capability or threshold established collaboratively by the requirements sponsor and the capability developer, changes to which could critically impact the effectiveness and survivability of the proposed system.

2.5.2.3.2. Summarize any information generated from an internal threat compromise IAW a Classified Information Compromise Assessment (CICA) that may affect the current capability requirement being proposed in the CDD including the approved mitigation plan.

2.5.2.3.3. Include summaries of all applicable threats cited in the System Survivability (SS) KPP (i.e., Kinetic, CBRN, Space, EMS, and Cyber) if the operational context requires operation in such environments. These summaries will form the basis for a risk-managed approach to developing SS requirements.

2.5.2.4. Additionally, if the CDD is not based on a validated capability requirements document, provide the threat summary as outlined for Section 2 of an ICD.

2.5.3. Section 3: Capability Discussion.

2.5.3.1. The purpose of this section is to identify the validated capability requirements and associated capability gaps addressed by the CDD, and to outline the results of related studies or analysis performed since validation of the capability requirements.

2.5.3.1.1. Narrative in the capability discussion section, especially the discussion of dependencies, is to be consistent with DoDAF SV-8 generated during prior analysis, as modified for the scope and purpose of the CDD.

2.5.3.1.2. Provide updated DoDAF CVs consistent with the CDD.

2.5.3.2. Summarize all related analyses and/or studies conducted to derive the performance attributes (KPPs, KSAs, and APAs) presented later in the CDD. Ensure the summary includes any intelligence analyses considered. Include the alternatives, objective, criteria, assumptions, recommendations, and conclusion. Ensure that final reports, or other resulting products, of studies or analyses not already present in KM/DS are uploaded for Reference purposes.

2.5.3.2.1. Provide a table that depicts the contribution this CDD makes to the fulfillment of capability requirements and closing of capability gaps described in the applicable ICDs, as illustrated in Figure B-5.

Capability Requirements			**Significant Gap(s)/Overlap(s)**	**CDD Contribution**
	Operational Attribute[1]/Metric	**Initial Objective Value**		
1. Capability Requirement			Briefly describe the most significant gap(s) and or overlap(s) for the requirement	**List Source ICD**
	Attribute 1.1	Value (no TBDs)		Identify KPP, KSA, or APA that addresses this requirement
	Attribute 1.n	Value (no TBDs)		Identify KPP, KSA, or APA that addresses this requirement
2. Capability Requirement			Sponsors should limit this to one sentence; preferably less than 15 words.	**List Source ICD**
	Attribute 2.1	Value (no TBDs)		Identify KPP, KSA, or APA that addresses this requirement
	Attribute 2.n	Value (no TBDs)		Identify KPP, KSA, or APA that addresses this requirement
n. Capability Requirement			See above	**List Source ICD**
	Attribute N.1	Value (no TBDs)		Identify KPP, KSA, or APA that addresses this requirement
	Attribute N.n	Value (no TBDs)		Identify KPP, KSA, or APA that addresses this requirement

Note:
[1] Attribute information is located in Annex A to Appendix B of Enclosure C of this manual starting on page C-B-A-1.

Figure B- 5: CDD Capability Requirement to Performance Attribute Traceability

2.5.3.2.2. Sponsors shall provide traceability between each capability requirement the proposed solution is addressing and the performance attribute (KPP, KSA, or APA) specified in Section 5 of the CDD.

2.5.3.3. Capability Dependencies. The DoDAF SV-8 captures all external dependencies between the capability solutions articulated in the CDD and fielded and planned capability solutions, including interactions with intelligence capabilities where appropriate over time. This provides insight into

the evolution of dependencies and enablers over the planned lifecycle of the capability solution.

2.5.3.3.1. Use the narrative in this section to discuss critical dependencies, and those with known risks or other issues.

2.5.3.3.2. In SoS capability solutions, the Sponsor is responsible for ensuring that related capability solutions identified in other CDDs and DCRs, remain compatible and that the development is synchronized. These related capability solutions tie to a common ICD or set of ICDs. In cases where development of SoS capability solutions involves multiple solution Sponsors, a lead Sponsor will be identified in the associated JROCM whom will coordinate efforts across organizations.

2.5.3.4. Address whether the capability solution will be subject to any undeveloped intelligence technologies or will be affected by the deactivation of fielded intelligence programs. Consider whether this will affect the effectiveness and timely delivery of the capability solution or increment. Ensure all timeframes for any enabling or program-required/dependent intelligence capabilities (fielded and future) are consistent with the capability solution's development schedule and planned IOC and FOC.

2.5.3.5. Additionally, if the CDD is not based on a validated capability requirements document, provide the capability requirements and associated capability gap information outlined for Section 3 of an ICD in addition to the content outlined in this section.

2.5.4. Section 4: Program Summary.

2.5.4.1. The purpose of this section is to outline the overall approach for developing capability solutions to satisfy validated capability requirements and associated capability gaps and to identify related interdependencies that must be satisfied to provide a successful capability solution.

2.5.4.2. Provide a summary of the overall program strategy for reaching FOC and, if applicable, the relationship between increments defined in the CDD. Carefully address the considerations (e.g., technologies to be developed, other systems in the FoS or SoS, inactivation of legacy systems) relevant to the incremental delivery plan. For follow-on increments, provide an update on the acquisition status of previous increments. Discuss any updates to the program strategy to reflect knowledge gained from previous increments, changes in approved Service or Joint Concepts, changes to CONOPS, or changes to the solution architecture or the DoD Information Enterprise Architecture (IEA).

2.5.4.3. Briefly describe whether the system being designed plans to use a Modular Open System Approach (MOSA) including integration of capabilities developed within the system and/or plan for evolution of capabilities that will be added, removed, or replaced in future increments.

2.5.4.4. Define what actions will constitute attainment of IOC and FOC of the current increment. Specify the target date for IOC and FOC attainment based

on discussions and coordination between the Requirement Sponsor and the acquisition community. Describe the types and quantities of required assets needed to attain IOC and FOC.

2.5.4.4.1. If the capability solution is intended to be integrated into one or more host platforms (such as for munitions or radios), then Sponsors should define the integration requirements and timing in the definitions of IOC and FOC in this section. This is the preferred approach rather than trying to define what the threshold and objective platform requirement is in Section 5 of the CDD.

2.5.4.4.1.1. Multiple sets of IOC and FOC dates may be defined to identify "lead" and "following" integration platforms.

2.5.4.4.1.2. If all intended integration platforms need to be available to the warfighter on the same schedule, then the Sponsor should identify a single set of IOC and FOC dates.

2.5.4.4.1.3. If the Sponsor would like to preserve the option for future integration on additional platforms not currently planned or resourced, then the Sponsor should capture any integration limitations in the Other System Attributes Section of the CDD (Section 6).

2.5.4.4.2. Identify the operational units, including other DoD Components, government agencies, or allied/partner nations that will employ the capability solution, and define the required quantities for each organization. This information will leverage and be consistent with the DoDAF OV-4 generated during prior analysis and will be updated for the scope and purpose of the CDD.

2.5.4.4.3. Total quantities must include the operational inventory as well as required quantities for training, spares, scheduled repair, and anticipated attrition over the lifecycle. Initial production planning should be based on these quantities, and changes to it may trigger a JROC/JCB Tripwire review IAW Enclosure A of this manual.

2.5.5. Section 5: Performance Attributes. (KPPs, KSAs, or APAs)

2.5.5.1. The purpose of this section is to outline the performance attributes intended to satisfy the validated capability requirements and associated capability gaps.

2.5.5.1.1. Sponsors should avoid over specification or inclusion of technical specifications as performance attributes.

2.5.5.1.2. The narrative in this section is to be consistent with DoDAF CV-3, SV-7, and SV-8 generated during prior analysis, as modified for the scope and purpose of the CDD.

2.5.5.2. Correlate each performance attribute (KPP, KSA, or APA) to the operational attributes of the capability requirements defined in the ICD. The Sponsor should identify the lowest tier JCA possible for each attribute.

2.5.5.2.1. Ensure the parameters most critical to mission effectiveness are captured as KPPs.

2.5.5.2.2. If the CDD is describing multiple increments, clearly identify which performance attributes (KPPs, KSAs, or APAs) apply to each increment, and the development threshold/objective values for each. These may also be specified in the annex for each increment.

2.5.5.2.3. If degraded levels of performance are acceptable under certain mission environments or conditions, articulate separate threshold and objective values for the affected performance attributes.

2.5.5.2.4. If the CDD is describing an FoS solution, it must describe the performance attributes for the FoS level of performance as well as any unique performance attributes for each of the constituent systems.

2.5.5.2.5. Identify all performance attributes that are threat-sensitive and dependent upon intelligence resources or support. For performance attributes (KPPs, KSAs, and/or APAs) which are dependent upon IMD to perform as specified, ensure identification of IMD dependent attributes and any schedule or cost considerations for IMD. Reference Annex G to Appendix G of this enclosure for detailed information on what is required to address intelligence supportability.

2.5.5.3. Present each performance attribute (KPP, KSA, or APA) in terms of parameters needed to address the validated capability requirements consistent with the DoDAF CV-3.

2.5.5.3.1. The performance attributes reflect Measures of Performance (MOPs) for the system being developed and not Measures of Effectiveness (MOEs) in conducting the mission. Ensure parameters chosen are technically achievable, quantifiable, measurable, testable, unambiguous, supported by documented trade-off analysis, and defined in a manner that supports efficient and effective T&E (T&E).

2.5.5.3.2. Provide threshold values for each performance attribute that represent the value below which performance would require reevaluation of military utility in the applicable CONOPS and/or Operational Mode Summary/Mission Profile (OMS/MP). Provide objective values in cases where the increased performance level of a parameter provides significant increases in operational utility.

2.5.5.3.3. Provide a range between threshold and objective values to allow trade space to explore during the TMRR and EMD phase of acquisition without having to revalidate the CDD to pursue different levels of performance. The PM may use this information to provide incentives for the development contractor or to weigh capability tradeoffs between threshold and objective values. Trade space should be sufficient to allow for increased capability in the future due to evolving technology, threat, or interoperability needs.

2.5.5.4. Address the four mandatory KPPs (Energy, System Survivability, Force Protection, and Sustainment) and provide a summary table for the net-ready performance attribute, which depending upon the system can be determined to be a KPP, KSA, or APA.

2.5.5.4.1. For each mandatory KPP, provide attributes related to it that must be met rather than a generic statement that the certifications and/or endorsements will be obtained.

2.5.5.4.1.1. Under the SS KPP, identify the Cyber Survivability Risk Category (CSRC) and EMS Survivability Risk Category and how it was determined (for cyber, specify if the Cyber Survivability Endorsement Implementation Guide - recommended approach was used).

2.5.5.4.1.1.1. Include tailored language for the CDD for both Cyber Survivability and EMS Survivability, as applicable;

2.5.5.4.1.1.2. Address the Cyber Survivability Pillars (Prevent, Mitigate, and Recover from Cyber Attacks) and the associated Cyber Survivability Attributes (CSAs) (1-10), as applicable.

2.5.5.4.1.1.3. Provide in a table or, as needed, in the associated narrative.

2.5.5.4.1.1.4. Reference the Cyber Survivability Endorsement Implementation Guide and EMS Survivability Guidebook, via KM/DS (Reference [4]), for more information.

2.5.5.4.2. For net-ready, include the summary table that presents the net-ready performance attributes and their associated metrics in terms of a standardized framework and data sources to leverage when developing attributes and their threshold and objective values.

2.5.5.4.2.1. The net-ready performance attribute (KPP, KSA, APA) is required to be addressed by the Sponsor in Section 7 (Joint Interoperability) of the CDD with the summary table captured in this section under either the KPP, KSA, or APA Tables as depicted in Figures B-6 through B-8.

2.5.5.4.2.2. For more information, see Annex A of Appendix G to this enclosure.

2.5.5.4.3. Neither the mandatory KPPs nor the net-ready performance attribute are applicable to every capability requirement. If the Sponsor determine that a mandatory KPP or the net-ready performance attribute is not applicable to their operational context, the Sponsor must articulate the reason(s) why.

2.5.5.4.4. Exclusion of a mandatory KPP or the net-ready summary table is subject to the approval authority of the certifying or endorsing organization as identified in Enclosure A of this manual. Early coordination with the appropriate certifying or endorsing organization for proposals to exclude a mandatory KPP or the net-ready summary table is essential to avoiding staffing delays.

2.5.5.5. Provide tables summarizing performance attributes in threshold and objective format, as illustrated in Figure B-6 through Figure B-8. If detail associated with each performance attributes (KPP, KSA, and APA) cannot be adequately captured within the tables, additional detail may be provided in separate numbered subparagraphs.

2.5.5.5.1. Check the box for any KPPs recommended to be JPRs. The Joint Staff Gatekeeper will review all Sponsor recommended JPRs along with all other KPPs, KSAs, and APAs and will approve the designation of JPRs. This JS Gatekeeper's JPR designation will be strongly influenced by the recommendation given by the Sponsor, the Lead FCB, and other advisors such as the certification and endorsement organizations.

Tier 1 to 3 JCAs	Key Performance Parameter	JPR (check box)	Threshold	Objective
	KPP 1	☐	Value	Value
	KPP 2	☐	Value	Value
	KPP 3	☐	Value	Value

Figure B- 6: KPP Table Format

Tier 1 to 3 JCAs	Key System Attribute	Threshold	Objective
	KSA 1	Value	Value
	KSA 2	Value	Value
	KSA 3	Value	Value

Figure B- 7: KSA Table Format

Tier 1 to 3 JCAs	Additional Performance Attribute	Threshold	Objective
	APA 1	Value	Value
	APA 2	Value	Value
	APA 3	Value	Value

Figure B- 8: APA Table Format

2.5.6. Section 6: Other System Attributes.

2.5.6.1. The purpose of this section is to identify any other system attributes not directly quantified (as performance attributes) and traceable to operational performance, and not identified elsewhere in the document.

2.5.6.2. Other system attributes may include the following:

2.5.6.2.1. Future integration platforms. Used in cases where integration on certain platforms is not currently planned or resourced, not already captured in the IOC and FOC definitions in the Program Summary Section of the ICD (Section 4), but the Sponsor would like to preserve the option for future integration on additional platforms.

2.5.6.2.2. Embedded instrumentation, electronic attack, and wartime reserve mode (WARM) requirements.

2.5.6.2.3. Human Systems Integration (HSI) considerations that have a major impact on system effectiveness and suitability.

2.5.6.2.4. Natural environmental factors, including climatic design type, terrain, meteorological and oceanographic (METOC) factors, impacts, and effects.

2.5.6.2.5. Physical and operational security needs, including technology security, foreign disclosure, defense exportability features, and anti-tamper.

2.5.6.2.6. Weather, oceanographic and astro-geophysical support needs throughout the program's projected lifecycle, including data accuracy and forecast needs.

2.5.6.2.7. Transportability and deployability considerations, IAW Reference [38], will include how the capability solution and related materiel will be moved either to or within the theater, and identify any lift limitations.

2.5.6.2.8. Space, Weight, & Power, and Cooling (SWAP-C) margin requirements and open system attributes, to ensure future flexibility and upgradability of systems and sub-systems to changing technologies and threats.

2.5.6.2.9. Derived system requirements to support systems that may be used in allied, partner-nation, coalition, or multinational operations relating to U.S.-ratified international standardization agreements, IAW References [38], [39], [40], and [41].

2.5.6.2.10. Cybersecurity Risk Management for DoD IT Systems: In addition, the CDD should identify the system categorization for information systems and Platform IT (PIT) systems as a required capability — the potential impact (low, moderate, or high) resulting from loss of confidentiality, integrity, and availability if a security breach occurs.

2.5.7. Section 7: Joint Interoperability.

2.5.7.1. The purpose of this section is to specify how the individual system will interoperate within the joint environment including any physical or net-ready interoperability effects on joint operations or operations with allies and partners. Additionally, Sponsors should include information that may enhance innovation such as the use of MOSA to support future incremental development. Any information on MOSA provided in this section should be in-sync with Section 4 (Program Summary) of the CDD and the PM's acquisition strategy, and briefly describe any considerations that may affect a future system or subsystem's interoperability with the base system (e.g., inclusion of system interfaces that support one or many consumer/producer systems and are compliant with consensus-based standards).

2.5.7.2. If applicable, Sponsors will address intelligence interoperability requirements consistent with Annex G to Appendix G to this enclosure.

2.5.7.3. Physical Interoperability. The Sponsor should describe the physical aspects of joint interoperability that may impact the capability solution proposed. This description must be consistent with the OV-2 in describing resources flows to and from the proposed capability, and further described in

the SV-1 to describe what enacts the OV-2 flow, now (as-is) or in the future. The Sponsor should use this section to describe any physical requirements (i.e., required landing space, runway length, etc.) that may impact the joint force. Additionally, the Sponsor should use this section to describe any SoS or FoS considerations for the proposed capability solution.

2.5.7.4. Net-Ready Interoperability. (Reference the Net-Ready Guide in Annex A to Appendix G to this enclosure). Net-Ready Interoperability shall be discussed as described in Annex A to Appendix G of this enclosure. If applicable, Sponsors must include a summary table in Section 5 of the CDD (Reference Paragraph 2.5.5.5. of this manual) that presents the net-ready performance attributes and their associated metrics in terms of a standardized framework and data sources to leverage when developing attributes and their threshold and objective values. Threshold and objective performance values should be represented in numerical form whenever possible to preclude subjective interpretation. Figure B-9 represents the required format for the net-ready performance attribute summary table for the CDD.

NR Performance Attribute	Performance Parameter[1]	Threshold[1]	Objective[1]
Support to Military Operations	**Mission:** *SQC Mission is to plan, request, coordinate, and control Close Air Support (CAS) missions, and provide C2 situational awareness, in support of joint and coalition ground maneuver forces.* **Mission Activity:** *Provide voice and data communications with mission partners.* **Measure:** *Accuracy of SQC information; consistently processed, stored, and made available to user or external consumer exactly as obtained.* **Mission Activity:** *Provide situational awareness* **Measure:** *Accuracy of mission update messages from other C2 platforms.* **Conditions:** *Adverse weather, day/night air transport operations in permissive to low threat environment.*	 *≥ 99%* *≥ 99%*	 *≥ 95%* *≥ 95%*
Enter and Manage in the Network	**Network**: *NIPRNET.* **Measure:** *Time to connect to an operational network from power up.* **Network**: *SIPRNET.* **Measure:** *Time to connect to an operational network from power up.* **Network**: *Link-16.* **Measure:** *Time to connect to an operational network from power up.* **Measure:** *Availability of network during adverse weather conditions.*	*≤ 1 minute* *≤ 5 minutes* *≤ 2 minutes* *≥ 99%*	*≤ 30 seconds* *≤ 1 minute* *≤ 1 minute* *≥ 97%*

NR Performance Attribute	Performance Parameter[1]	Threshold[1]	Objective[1]
	Condition: *Continuous Network Connectivity based on system-controllable factors.*		
Exchange Information	**Information Element:** *Support Data.* **Measure:** *Time to exchange data between SQC and System A (NGA).*	*≤ 2 minutes*	*≤ 1 minute*
	Information Element: *Target Data.* **Measure:** *Time to exchange data between SQC and System B (NSA).*	*≤ 2 minutes*	*≤ 1 minute*
	Information Element: *ISR Data.* **Measure:** *Time to exchange data between SQC and System C (USCENTCOM).*	*≤ 2 minutes*	*≤ 1 minute*
	Conditions: *NSA Type 1 Certified Encryption Systems in operation and continuous network connectivity.*		
Note: [1] **Bold text is the template**; *non-bold italicized text provides an example*.			

Figure B- 9: Net-Ready Performance Attribute CDD Example

2.5.7.5. Joint Training Technical Interoperability. For systems with a mission solely focused on training, exercises, and/or mission rehearsal, specify how these systems will interoperate within the joint training enterprise, including effects on joint training operations with allies and partners. Also, state the intent to design these systems to Joint Training Technical Interoperability standards and common technical approaches for interoperability. Joint Training Technical Interoperability Standards and Technical Approaches are maintained in the DoD IT Standards Registry (DISR) and, as appropriate, the Defense Standardization Program's Acquisition Streamlining and Standardization Information System (ASSIST).

2.5.8. Section 8: Spectrum and Electromagnetic Environmental Effects Control Requirements.

2.5.8.1. The purpose of this section is to identify electromagnetic (EM) spectrum and electromagnetic environmental effects (E3) control requirements and to ensure compliance with appropriate policy and guidance. This information also informs the net-ready review and certification conducted during staffing of the CDD as well as support compliance with System Survivability KPP and Force Protection KPP.

2.5.8.2. All spectrum dependent programs/systems must comply with the spectrum management and (E3) direction. The spectrum supportability process includes joint, DoD, national and international policies and procedures for the management and use of the EM spectrum. The spectrum supportability process is detailed in Annex A to Appendix G to this enclosure with details on compliance available at References [42], [43], and [44]. IAW Reference [44], spectrum certification, Host Nation coordination/approval, and spectrum

supportability risk assessment (SSRA) requirements should be addressed/summarized in this paragraph.

2.5.8.3. All electrical and electronic systems, subsystems, and equipment, including ordnance, must comply with E3 direction IAW Reference [59]. Summarize in this section the requirements to ensure mutual electromagnetic compatibility (EMC) and effective E3 control in its electromagnetic environment (EME). Requirements to control E3 shall consider all applicable E3 disciplines including EMC, electromagnetic vulnerability (EMV), electromagnetic pulse (EMP), electronic protection (EP), electrostatic discharge (ESD), and hazards of electromagnetic radiation to personnel (HERP), ordnance (HERO), and fuel (HERF).

2.5.8.4. Other applicable spectrum related requirements that may be included in this paragraph include bandwidth, quality of service, and spectrum data capture requirements for DoD by DoD and Federal spectrum certification as described in Reference [48]. If the capability will interface with JWICS or other intelligence-managed dissemination systems to receive or transmit information, bandwidth requirements and quality of service requirements must be addressed. Furthermore, ensure consistency with any identified intelligence interoperability requirements consistent with Annex G to Appendix G of this enclosure. If there are potential issues regarding E3 interference from threat emitters, ensure these issues are identified in this section. Ensure this section is consistent with the threat discussion in Section 2 of the CDD and in the DIA- or Service-approved threat products including, but not limited to, the VOLT report.

2.5.9. Section 9: Intelligence Supportability. (Reference the Intelligence Supportability Guide in Annex G to Appendix G to this enclosure)

2.5.9.1. The purpose of this section is to identify intelligence support requirements and to ensure compliance with appropriate IC policy and guidance. This information also informs the intelligence review and certification conducted during staffing of the CDD.

2.5.9.2. Identify, as specifically as possible, all intelligence support requirements throughout the projected lifecycle IAW Annex G to Appendix G of this enclosure.

2.5.9.3. Programs will be reviewed by the community, including DIA and J-283/IRCO, for IMD dependency. IMD dependent programs will be required to develop an LMDP IAW Reference [45]. Intelligence certification will include DIA evaluation and approval of actionable IMD requirements derived from the LMDP.

2.5.10. Section 10: Weapon Safety Assurance. (Reference the Weapons Safety Guide in Annex H to Appendix G to this enclosure.)

2.5.10.1. The purpose of this section is to ensure compliance with appropriate weapon safety policy and guidance, and when appropriate, to document

tailoring of weapon safety requirements driven by unique aspects of the operational context. This information also informs the weapon safety review and endorsement conducted during staffing of the CDD.

2.5.10.2. IAW Reference [46], all munitions capable of being used, packaged, handled, stored, or transported by any Service in joint warfighting environments are considered to be joint weapons and require a joint weapons safety review and Weapon Safety Endorsement (WSE) IAW Annex H to Appendix G of this enclosure and References [46] and [47]. See Annex H to Appendix G of this enclosure for baseline weapon safety requirements and additional guidance on setting tailored weapon safety requirements if required.

2.5.11. Section 11: Technology Readiness.

2.5.11.1. The purpose of this section is to highlight known technological challenges which may impact the ability to reach the level of performance identified in the performance attributes (KPPs, KSAs, or APAs), or represent risk to delivering capabilities on schedule and within budget. This information may be used to inform lifecycle cost, performance, schedule, and quantity tradeoff discussions during review and validation of the CDD.

2.5.11.1.1. For the CDD generated prior to the Milestone B acquisition decision, this section identifies technological risk areas that require attention during the EMD phase of acquisition.

2.5.11.1.2. In cases where the CDD describes multiple increments of a capability solution, this section must describe the critical technologies to be matured for each increment. This may also be addressed in the incremental annex as they are developed for a capability solution.

2.5.11.2. For each critical technology, discuss potential workarounds to achieve partial or complete program success in the event that the technology does not mature as anticipated. Additionally, highlight how incremental acquisition strategies and/or MOSA is being used to enable flexibility in critical technology areas. Where known, include decision points and criteria for implementing the potential workaround(s).

2.5.12. Section 12: DOTmLPF-P Considerations. (Reference the DOTmLPF-P Guide in Annex F to Appendix G to this enclosure)

2.5.12.1. The purpose of this section is to outline DOTmLPF-P changes that are required to successfully implement the materiel capability solution. This information also informs the DOTmLPF-P review and endorsement conducted during staffing of the CDD.

2.5.12.2. Sponsors must address all DOTmLPF-P considerations in a CDD unless not applicable. In cases where one or more of the DOTmLPF-P factors may not be applicable, the Sponsor shall coordinate with the applicable organization identified in Annex F to Appendix G of this enclosure to ensure the DOTmLPF-P endorsement is not withheld due to missing information. For

CDDs describing multiple increments, all DOTmLPF-P considerations that are increment dependent must be clearly identified.

2.5.12.3. Discuss any DOTmLPF-P changes associated with fielding the system, including those approaches that would impact Service and Joint Concepts, CONOPS, or plans within a CCMD Area of Responsibility (AOR), including any changes associated with the mitigation of risks of known intelligence shortfalls. Describe the implications for all recommended changes.

2.5.12.4. DOTmLPF-P changes are considered from two perspectives:

2.5.12.4.1. Enabling - changes that enable the implementation, operations, and support of the system;

2.5.12.4.2. Integrating - changes that must be made to support integration of this system with fielded capability solutions.

2.5.12.5. Include each of the DOTmLPF-P areas impacted by the capability solution addressed in the CDD. For DOTmLPF-P changes already addressed in separate DCRs, cite the DCR that applies and provide status. For DOTmLPF-P changes not already addressed in separate DCRs, provide details of the recommended changes and implementation plans in the following areas:

2.5.12.5.1. Doctrine - Identify changes to joint doctrine that may be required to fully implement the capability solution.

2.5.12.5.2. Organization - Identify changes to organizational structures that may be required to fully implement the capability solution.

2.5.12.5.3. Training.

2.5.12.5.3.1. Specify non-materiel considerations related to training required to fully realize the operational utility of the system. Outline changes or updates to current training practices that enable a new system to replace a legacy system. Training implications must be addressed from the beginning of the acquisition process, integrated with the planning, materiel development, and production, and updated throughout the capability solution's lifecycle.

2.5.12.5.3.2. In cases where the mission of the system is training, or operational context requires the warfighter to dictate materiel training requirements or approaches, the Sponsor should include training performance attributes (KPPs, KSAs, and/or APAs) in Section 5 (Performance Attributes) of the CDD.

2.5.12.5.4. Materiel - Identify materiel items, systems, or equipment needed to support the required capability. Materiel refers to increased quantities, modifications, improvements, or alternate applications of existing materiel or the purchase of commercial off-the-shelf (COTS), government off-the-shelf (GOTS), or non-developmental items (NDI).

2.5.12.5.5. Leadership and Education. Identify changes to leadership and education programs that may be required to ensure personnel are capable of fully implementing the capability solution.

2.5.12.5.6. Personnel. Identify changes to personnel quantities, types (officer, enlisted, civilian, and/or contractor), and skill sets required to fully implement the capability solution.

2.5.12.5.7. Facilities. Specify facility, shelter, supporting infrastructure, and ESOH asset requirements, and the associated lifecycle costs, availability, and acquisition milestone schedule(s) related to supporting the system. Detail any basing needs (forward and main operating bases, institutional training base, and depot requirements).

2.5.12.5.8. Policy. Identify changes to policy that may be required to fully implement the capability solution.

2.5.13. Section 13: Program Affordability.

2.5.13.1. The purpose of this section is to identify the overall resources associated with pursuing the capability solution, including materiel and non-materiel costs over its projected lifecycle, and to ensure those resources are planned to be available for successful execution of the program.

2.5.13.2. Cite the affordability caps from the acquisition program baseline for unit production and sustainment costs. This information informs lifecycle cost, performance, schedule, and quantity tradeoff discussions. Lifecycle cost data for all increments described in the CDD must be included in this section. Cost estimation used in CDDs shall be consistent with methods outlined in Reference [5].

2.5.13.3. Cite applicable lifecycle cost analyses, conducted IAW Reference [48], including other cost models that may include other U.S. Government agency/department or exportable-based business cases to reduce DoD lifecycle costs. Ensure that resource estimates have been reviewed by the Sponsor's cost analysis organization to ensure best practices are being followed. Ensure any final reports or other results documentation is uploaded into KM/DS for reference purposes.

2.5.13.4. Show projected lifecycle costs and acquisition quantity as shown in Figure B-10, including cost by fiscal year and type of funding based on threshold levels of performance. Show cost factors used to determine ACAT level per Reference [5]. Present key results from sensitivity and uncertainty analyses, including the confidence levels associated with resource estimates, based on the program's current level of knowledge. The affordability determination is made as part of the lifecycle cost assessment in the analysis supporting the CDD development which may include updates to earlier cost analyses. Ensure that lifecycle cost in the CDD includes all associated DOTmLPF-P and intelligence support considerations.

Acquisition Required Resources[1]									
BY$$[2]	FYxx (Current)	FYDP						Post-FYDP (FYyy-FYzz)	To Complete (FYxx-FYzz)
		FYxx+1	FYxx+2	FYxx+3	FYxx+4	FYxx+5	FYDP Total		
RDT&E									
Procurement									
MILCON									
O&M (Acq)									
MILPERS (Acq)									
Total (Acq)									
Acq. Quantity									

Warfighter Required Resources for System Operations and Support[3]					
BY$$[2]	Pre-IOC Ops (FYxx-FYaa)	IOC to FOC Ops (FYaa-FYbb)	Post-FOC Ops (FYbb-FYcc)	Operational Life (FYxx-FYcc)	**Notes:** [1] Current year is FYxx. First post-FYDP year is FYyy. End of planned production run is FYzz. [2] All resources normalized to a standard base year reference - BY$$. [3] Planned IOC is FYaa. Planned FOC is FYbb. Planned end-of-life is FYcc.
O&M (Ops)					
MILPERS (Ops)					
Total (Ops)					

Figure B- 10: Summary of Required Resources

2.5.13.5. In a similar manner to what is required by References [5], [49], and [50], describe how the resources outlined in Figure B-10 are affordable under the limitations of the Component's expected Total Obligation Authority (TOA) over a 30-year timeframe, including identification of legacy capabilities which will be reduced in scope or eliminated to allow funding of the proposed new capability. The 30-year "sand chart" data will be generated using the same OSD inflator values used to comply with affordability in Reference [5], and will be provided within the CDD or as supplemental data uploaded to the KM/DS system.

2.6. Appendices. Only the following appendices are allowed in the document. Additional reference documents or data may be submitted IAW procedures outlined in Enclosure A of this manual.

2.6.1. Appendix A. References. Ahead of other references provided in this appendix, the architecture must be discoverable and accessible IAW Appendix H to this enclosure and the architecture data and associated artifacts/views identified in Figure A-4 and, if applicable, Figure B-20 must also be discoverable.

2.6.2. Appendix B. Acronym List. List in alphabetical order, all of the acronyms used in the document.

2.6.3. Appendix C. Glossary. As the Sponsor develops the document glossary, they may leverage applicable definitions from the DoDAF AV-2. These do not

have to be identical, as some terms will only apply to the document or the DoDAF architecture; however, terms that apply to both must be consistent.

2.6.4. Appendix D. (Optional) Classified Appendix. A classified Appendix may be used in cases where only a small subset of the document needs to be protected at a higher classification level. If the document is not useful without this appendix, the document is to be classified at a higher level. A classified appendix's content will count toward the document body page limits and will be indexed to align with the baseline document sections. Except where the existence of classified content cannot be acknowledged, each section of the baseline document augmented by the classified Appendix will refer the reader to the classified appendix. If used, the appendix shall be provided to the Joint Staff Gatekeeper or J-8, Special Access Program Coordinator (J-8/SAPCOORD) IAW the classification of the appendix.

2.7. Annexes A – Z. (Optional) Incremental Approach or FoS. Sponsors may attach annexes to a CDD to define incremental capabilities or a FoS associated with a base CDD. See Annex A to this appendix for additional detail.

ANNEX A TO APPENDIX C TO ENCLOSURE B
INCREMENTAL CDD ANNEXES

1. Overview.

1.1. Purpose. The purpose of the incremental or FoS annexes is to provide the Sponsor with flexibility to redefine capabilities from a base document.

1.2. Applicability. These annexes are applicable to all CDDs at the Sponsor's discretion.

1.2.1. Incremental Development Approach. In an incremental development approach for capabilities, a Sponsor shall specify the capability solution in a base CDD. As incremental capability is added to the base system over time, or block upgrades are developed, the Sponsor shall document this in an annex to the base CDD.

1.2.1.1. Unless specified in an annex, the increments inherit the attributes of the base system that is specified in the initial CDD.

1.2.1.2. It is likely the incremental approach will span several years as new technology matures; however, the Sponsor must remain within the general scope outlined in the base CDD and address approved joint military capabilities as specified in an ICD.

1.2.1.3. For programs generating variants of the base capability to fill additional gaps, the principles of the incremental approach apply.

1.2.1.4. The annex will be staffed through the deliberate process, unless tailored staffing is requested through and approved by the Joint Staff Gatekeeper. As these documents will be separate by time, the base CDD must accompany the annex through the staffing process; however, stakeholders are only to provide comments and validation of the annex.

1.2.2. FoS Approach. In a FoS approach, the Sponsor shall develop a base CDD and concurrently staff annexes for individual systems within the family. The base CDD will specify attributes for the entire FoS and each annex will specify additional attributes for the individual systems.

1.2.2.1. The individual systems in a FoS approach inherit the attributes of the base CDD.

1.2.2.2. The annex will be staffed along with the base document and the validation authority may validate the entire FoS or individual annex as part of the FoS.

1.2.2.3. Although it is likely that in this approach the annex will be staffed concurrently; a Sponsor may develop a FoS over time in a similar manner to the incremental approach.

1.2.2.4. Sponsors will ensure each individual system within the family remains in context with the base CDD and meets approved joint military capabilities as specified in an ICD.

1.3. Proponent. The proponent for this annex is the J-8/JCD. For questions, contact J-8/JCD at (703) 695-2705.

2. Annex Content Guide. Each individual annex will include the same sections as a CDD. Sections with no change to base document must be present but can state "No Change." Individual annexes are not to exceed 20 pages in length.

2.1. Format.

2.1.1. Section 1: Operational Context. Provide updates to operational context described in the base CDD.

2.1.2. Section 2: Threat Summary. Provide updates to threat summary or threat documents specified in the base CDD.

2.1.3. Section 3: Capability Discussion. Specify capabilities developed for the individual annex.

2.1.4. Section 4: Program Summary. Provide updates to the program summary. If an incremental approach is taken, describe the strategy taken to deliver the incremental capability.

2.1.5. Section 5: Development of Performance Attributes. Specify performance attributes specific to the increment or the individual system within the family. The capability solution specified by the annex will be a subset of what is required to meet the performance attributes of the overall system as identified in the base document.

2.1.6. Section 6: Other System Attributes. Specify other system attributes specific to the increment or the individual system within the family. The capability solution specified by the annex inherits the attributes of the base document.

2.1.7. Section 7: Joint Interoperability. Specify how the individual system or increment will interoperate within the joint environment. In the incremental approach, Sponsors shall ensure the incremental capability meets the current standards at the time of validation. It is likely a new net-ready summary table will be required for each increment or individual system in an FoS. If applicable, the Sponsor will also update the intelligence interoperability requirements consistent with Annex G to Appendix G to this enclosure.

2.1.8. Section 8: Spectrum and E3 Control Requirements. Capture any additional spectrum and E3 control requirements for the increment or individual system.

2.1.9. Section 9: Intelligence Supportability. Capture changes to the requirements or additional supportability requirements from the base document.

2.1.10. Section 10: Weapon Safety Assurance. Outline any changes from the base document.

2.1.11. Section 11: Technology Readiness. Specify the technology readiness of the capability for the increment or individual system.

2.1.12. Section 12: DOTmLPF-P Considerations. Describe any additional DOTmLPF-P considerations for the increment of individual system.

2.1.13. Section 13: Program Affordability. Specify any updates to the base document.

2.2. Validation. These annexes must be validated by the validation authority for the base document as specified by the JSD. Sponsors cannot attach additional annexes without validation by the designated validation authority.

2.2.1. In an incremental development approach, each annex may require individual validation by the validation authority of the base CDD. If these are submitted over time, the Sponsor shall submit the base CDD along with the annex, but only the annex will be validated by the validation authority.

2.2.2. In a FoS approach, several annexes may be submitted with the base document and all annexes will be validated with the base document. If additional systems in the family are submitted for validation, they must be individually validated in a similar fashion to the incremental approach.

2.2.3. Sponsors who wish to submit incremental or FoS annexes should consult with the Joint Staff Gatekeeper prior to pursuing this approach. The Joint Staff Gatekeeper may reject an annex if it is outside the scope of the base document.

APPENDIX D TO ENCLOSURE B

IS-CDD

1. Overview. The IS-CDD is a variant of the regular CDD, implementing the "IT Box" construct outlined in this section. IS-CDDs streamline the requirements process by delegating oversight and formats for subsequent documents as identified in the IS-CDD. This provides IS programs greater flexibility to incorporate evolving technologies and achieve faster acquisition.

1.1. Purpose. The purpose of an IS-CDD is to facilitate efficient and timely software development efforts; IS-CDDs are not appropriate for hardware development efforts or capturing capability requirements that span a broad scope of hardware, software, and/or DOTmLPF-P efforts. The IS-CDD serves as the basis for validation by the validation authority identified in Enclosure A of this manual. Any streamlining of acquisition processes is at the discretion of the MDA IAW References [5] and [9].

1.2. Applicability.

1.2.1. IS-CDDs are appropriate in the same situations as an IS-ICD with the exception that an IS-CDD happens when an IS solution is identified in an AoA as a follow-on to a traditional ICD as the Sponsor follows the deliberate JCIDS path.

1.2.2. IS-CDDs are not appropriate in the same situations as an IS-ICD.

1.2.3. See the IS-ICD format section under Appendix B to Enclosure B of this manual for more information on IS-ICD formats.

1.2.4. In cases where the potential for use of the "IT Box" construct is unclear or in dispute, the Joint Staff Gatekeeper, in consultation with the validation authority as needed, will determine whether an CDD or IS-CDD will be used.

1.2.5. Joint command and control (C2) requirements that have a validated IS-CDD will be identified, documented, validated, prioritized, managed, and monitored IAW [11].

1.2.6. Biennial FCB Review of IS Systems. For all IS programs with a valid IS-CDD, the Lead FCB shall review an update every second year following the validation. The Lead FCB will determine if the JROC or JCB should review the following items and will make appropriate recommendations for action.

1.2.6.1. Progress in delivering capability solutions within the required timeframe and available funding.

1.2.6.2. Compliance with applicable EA and data standards.

1.2.6.3. Other items as identified by the IS-CDD validation.

1.3. Proponent. The proponent for this appendix is the J-8/JCD. For questions, contact J-8/JCD at (703) 695-2705.

2. Format.

2.1. Cover Page. The cover page for an IS-CDD shall be the same as for a regular CDD except that the title will begin with the phrase "Information Systems Capability Development Document for…"

2.2. Validation Page. No change from a regular CDD to the validation page for an IS-CDD.

2.3. Waivers (if applicable). No change from a regular CDD to the waiver section for an IS-CDD.

2.4. Executive Summary. No change from a regular CDD to the executive summary in the IS-CDD.

2.5. Document Body. The body of an IS-CDD differs from a regular CDD in six sections, one section is optional, and removes the requirement for one section. The document shall be no more than 45 pages long including any content modified or augmented by a classified Annex, if used. See the regular CDD section for content of the unchanged sections.

2.5.1. Section 1: Operational Context. No change from a regular CDD to the operational context section in the IS-CDD.

2.5.2. Section 2: Threat Summary. No change from a regular CDD to the threat summary of the IS-CDD; however, the Sponsor should strongly consider the cyber threats posed to an IS solution.

2.5.3. Section 3: Capability Discussion. Same as the regular CDD with the exception of the following:

2.5.3.1. Provide a table that briefly describes the contribution this IS-CDD makes to the fulfillment of capability requirements described in the applicable ICDs or analysis of the capability gaps as illustrated in Figure B-11.

Capability Requirements			Significant Gap(s)/Overlap(s)	IS-CDD Contribution
	Operational Attribute/Metric	Initial Objective Value		
1. Capability Requirement			Briefly describe the most significant gap(s) and or overlap(s) for the requirement.	**List Source ICD**
	Attribute 1.1	Value (no TBDs)		Identify KPP, KSA, or APA that addresses this requirement
	Attribute 1.n	Value (no TBDs)		Identify KPP, KSA, or APA that addresses this requirement
2. Capability Requirement			Sponsors should limit this to one sentence; preferably less than 15 words.	**List Source ICD**
	Attribute 2.1	Value (no TBDs)		Identify KPP, KSA, or APA that addresses this requirement
	Attribute 2.n	Value (no TBDs)		Identify KPP, KSA, or APA that addresses this requirement
n. Capability Requirement			See above.	**List Source ICD**
	Attribute N.1	Value (no TBDs)		Identify KPP, KSA, or APA that addresses this requirement
	Attribute N.n	Value (no TBDs)		Identify KPP, KSA, or APA that addresses this requirement

Figure B- 11: IS-CDD Capability Requirement to Performance Attribute Traceability

2.5.4. Section 4: Program Summary. Same as the regular CDD with the addition to the following:

2.5.4.1. Development of the IT Box.

2.5.4.2. The “IT Box” construct, Figure B-12, calls for fewer iterations of validating capability requirements documents through the JCIDS process by describing the overall IS program and delegating validation of detailed follow-on requirement and solution oversight to a flag-level organization other than the JROC or JCB.

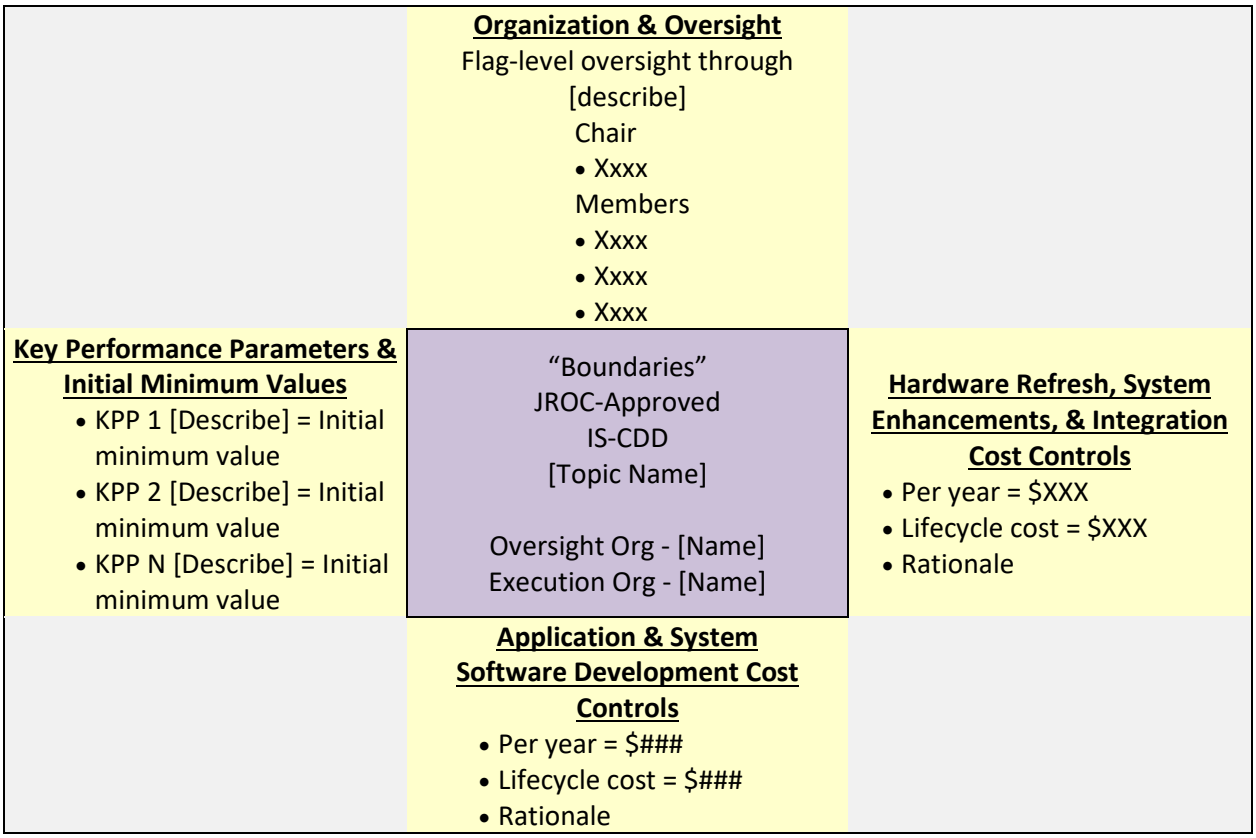

Figure B- 12: Components of the "IT Box" Construct in IS-CDDs

2.5.4.2.1. The IT Box model uses initial minimum values in place of initial objective values so that the baseline capability is clearly specified, and the delegated oversight body has flexibility to further develop capabilities without revalidation of the capability requirements document.

2.5.4.2.2. Initial minimum values represent the achievable level of required capability needed to incorporate current technology to meet the baseline capability.

2.5.4.2.3. Successor documents must be provided to the KM/DS system for information purposes and visibility in the capability requirements portfolios.

2.5.5. Section 5: Performance Attributes (KPPs, KSAs, and APAs). Follows the same format as a regular CDD with the exception of the following:

2.5.5.1. Performance attributes may be quantified in terms of initial minimum values rather than threshold/objective values. As with regular CDDs, the performance attributes must reflect performance that satisfies the capability requirements identified in Section 3 of the IS-CDD. Reference Figure B-13, under paragraph 2.5.7.1, of this manual as an example of how to capture the net-ready performance attributes for an IS-CDD.

2.5.5.2. Mandatory KPPs. Only two of the four mandatory KPPs apply to an IS-CDD. The System Survivability (SS) KPP and Sustainment KPP are required for the IS-CDD.

2.5.5.2.1. SS KPP. For an IS-CDD, the SS should focus on the ability of the system to operate in a cyber and EMS-contested environment as per Annex C to Appendix G of this enclosure. The following shall be included under the SS KPP:

2.5.5.2.1.1. Identify the Cyber Survivability Risk Category (CSRC), EMS Survivability Risk Category, and how they were determined (for Cyber, specify if it was determined using the CSEIG-recommended approach);

2.5.5.2.1.2. Include tailored language for the CDD (tailored for an IS-CDD);

2.5.5.2.1.3. Address the Cyber Survivability Pillars (Prevent, Mitigate, and Recover from Cyber Attacks) and the associated Cyber Survivability Attributes (CSAs) (1-10), as applicable. This information can be provided in a table or, as needed, in the associated narrative. For more information, see the CSE Implementation Guide, via KM/DS additional guidance.

2.5.5.2.1.4. For EMS Survivability, see Annex C to Appendix G of this enclosure and the EMS Survivability Guidebook, via KM/DS (Reference [4]).

2.5.5.2.2. Sustainment KPP. For an IS-CDD the Sponsor should focus the Sustainment KPP on the operational availability of the IS solution as per Annex D to Appendix G of this enclosure.

2.5.6. Section 6: Other System Attributes. Optional for an IS-CDD with the exception of consideration should be given to identify the system categorization for information systems and PIT systems as a required capability - the potential impact (low, moderate, or high) resulting from loss of confidentiality, integrity, and availability, if a security breach occurs IAW [12].

2.5.7. Section 7: Joint Interoperability. Same as the regular CDD with the exception of the following.

2.5.7.1. The summary table for the net-ready performance attribute will be slightly different from that of a CDD since it will be quantified in terms of initial minimum values rather than threshold/objective values. To illustrate this, reference Figure B-13 below.

NR Performance Attribute	Performance Parameter[1]	Initial Minimum Value
Support to Military Operations	**Mission:** *Security Qualitative Capability (SQC)[2] Mission is to plan, request, coordinate, and control Close Air Support (CAS) missions, and provide C2 situational awareness, in support of joint and coalition ground maneuver forces.* **Mission Activity**: *Provide voice and data communications with mission partners.* **Measure:** *Accuracy of SQC information; consistently processed, stored, and made available to user or external consumer exactly as obtained.* **Mission Activity**: *Provide situational awareness*	 *≥ 99%* *≥ 99%*

NR Performance Attribute	Performance Parameter[1]	Initial Minimum Value
	Measure: *Accuracy of mission update messages from other C2 platforms.* **Conditions:** *Adverse weather, day/night air transport operations in permissive to low threat environment.*	
Enter and Manage in the Network	**Network**: *NIPRNET.* **Measure:** *Time to connect to an operational network from power up.* **Network**: *SIPRNET.* **Measure:** *Time to connect to an operational network from power up.* **Network**: *Link-16.* **Measure:** *Time to connect to an operational network from power up.* **Measure:** *Availability of network during adverse weather conditions.* **Condition:** *Continuous Network Connectivity based on system-controllable factors.*	*≤ 1 minute* *≤ 5 minutes* *≤ 2 minutes* *≥ 99%*
Exchange Information	**Information Element:** *Support Data.* **Measure:** *Time to exchange data between SQC and System A (NGA).* **Information Element:** *Target Data.* **Measure:** *Time to exchange data between SQC and System B (NSA).* **Information Element:** *ISR Data.* **Measure:** *Time to exchange data between SQC and System C (USCENTCOM).* **Conditions:** *NSA Type 1 Certified Encryption Systems in operation and continuous network connectivity.*	*≤ 2 minutes* *≤ 2 minutes* *≤ 2 minutes*

Note:
[1] **Bold text is the template**; *non-bold and italicized text provides an example*.
[2] Security Qualitative Capability (SQC) is a fictitious program for the purposes of this template.

Figure B- 13: Net-Ready Performance Attribute IS-CDD Example

2.5.8. Section 8: Spectrum Requirements. No change from a regular CDD to the Spectrum Requirements section of the IS-CDD.

2.5.9. Section 9: Intelligence Supportability. No change from a regular CDD to the Intelligence Supportability section of the IS-CDD.

2.5.10. Section 10: Weapons Safety Assurance. Not required for an IS-CDD. By definition, an IS-CDD is not appropriate for developing munitions.

2.5.11. Section 11: Technology Readiness. This should verify the planned capability is aligned with current information technology levels and not dependent on technology development to achieve initial minimum values.

2.5.12. Section 12: DOTmLPF-P Considerations. No change from a regular CDD to the DOTmLPF-P Considerations section of the IS-CDD.

2.5.13. Section 13: Program Affordability. Follows the same format as a regular CDD with the exception of the following:

2.5.13.1. In place of the required resources table used in a CDD, identify the programmed funding by year for the software development and sustainment and for hardware refresh and integration, as shown in Figure B-14. Provide rationale for the level of funding required in the same manner as for a CDD.

Required Resources:									
BY$$[2]	**FYxx (Current)**	**FYDP**						**Post-FYDP (FYyy-FYzz)**	**Life Cycle Cost (FYxx-FYzz)**
		FYxx+1	**FYxx+2**	**FYxx+3**	**FYxx+4**	**FYxx+5**	**FYDP Total**		
Application and System Software Development Costs									
RDT&E[3]									
Procurement[3]									
MILCON[3]									
O&M[3]									
MILPERS[3]									
Total									
Hardware Refresh, System Integration									
RDT&E[4]									
Procurement[4]									
MILCON[4]									
O&M[4]									
MILPERS[4]									
Total									
Overall Total									

Notes:
[1] Current year is FYxx. First post-FYDP year is FYyy. End of planned capability life, or end of 30-year TOA projection if no planned service life, is FYzz.
[2] All resources normalized to a standard base year reference - BY$$.
[3] Application and System Software Development Costs.
[4] Hardware Refresh, System Integration Costs.

Figure B- 14: Example Life Cycle Cost Summary Table for IS-CDDs

2.5.13.2. Cite applicable lifecycle cost analyses, conducted IAW Reference [48], including other cost models that may include other U.S. Government agency/department or exportable-based business cases to reduce DoD lifecycle costs. Ensure that resource estimates have been reviewed by the Sponsor's cost analysis organization to ensure best practices are being followed. Ensure that any final reports or other results documentation is uploaded into KM/DS for reference purposes.

2.6. Appendices. The appendices for an IS-CDD are the same as for a regular CDD.

APPENDIX E TO ENCLOSURE B

JOINT DOTmLPF-P CHANGE RECOMMENDATION (DCR)

1. Overview.

Purpose. The purpose of a DCR (either Component-specific or Joint) is to propose non-materiel capability solutions, which may serve as an alternative to, or complement of, materiel capability solutions. Sometimes referred to as "little m" materiel, the materiel DOTmLPF-P consideration is everything necessary to equip DoD forces to operate effectively. The letter "m" in the acronym is usually lower case, since Joint DCRs do not advocate new materiel development, but rather advocate increased quantities or alternate applications of existing materiel to include Commercial Off-The-Shelf (COTS), Government Off-The-Shelf (GOTS), or Non-Development Items (NDI).

1.1. Applicability. The DCR (either Component-specific or joint) serves as the basis for validation by the appropriate validation authority identified in Enclosure A of this manual.

1.1.1. DoD Components manage Component-specific DCR at their discretion. Sponsors may use a DCR in support of non-materiel capability solutions or as enablers of materiel capability solutions IAW policies and processes of that organization.

1.1.2. For non-materiel solutions that impact more than just a single DoD Component, a Joint DCR is used to ensure equities of all effected organizations are addressed during review and validation. By definition, Joint DCRs have impact on the joint force and are assigned a JSD of JROC Interest or JCB Interest IAW Enclosure A of this manual.

1.2. Proponent. The proponents for this appendix are J-8/JCD. For questions, contact J-8/JCD at (703) 695-2705.

2. Format.

2.1. Cover Page. The cover page of a Joint DCR shall include the following information.

2.1.1. Classification.

2.1.2. Title, starting with the phrase "Joint DOTmLPF-P Change Recommendation for…"

2.1.3. Sponsoring organization, and signature authority who authorized the submittal for review and validation. New Joint DCRs, and modifications to validated Joint DCRs, must be endorsed by the Sponsor J-8 equivalent or higher.

2.1.4. Date submitted by the Sponsoring organization.

2.1.5. Primary and secondary POCs for the document Sponsor. Include name, title/rank, phone, and both NIPRNET and SIPRNET email addresses. POCs must have completed the appropriate level of RMCT IAW Reference [1].

2.1.6. Proposed lead organization. Designates a single organization, which may be different from the document Sponsor, which will have responsibility for coordinating the proposed changes. If applicable, coordinate the activities of other OPR change recommendations within the Joint DCR.

2.1.7. Document revision number.

2.2. Validation Page.

2.2.1. While a document is in draft, a placeholder page will be included, with the statement, "This document (include revision numbering) has not yet been validated and shall not be considered to be an authoritative source for the content herein. This document may be considered authoritative only when this page is replaced by a signed validation memorandum."

2.2.2. Once validated by the appropriate requirement validation authority, the placeholder page will be replaced by the signed validation memorandum.

2.2.3. If revisions to a document are proposed after validation, the placeholder page will be reinserted ahead of the original validation memorandum, until the updated validation memorandum is inserted. The original validation memorandum and memoranda validating subsequent changes, if applicable, are retained as part of the authoritative document.

2.3. Waivers (if applicable). In cases where the Sponsor was granted a waiver for format or content, a copy of the signed waiver or reference to the Joint Staff Gatekeeper's KM/DS approval note shall be included in the document so all stakeholders understand the divergence of the document from the JCIDS format.

2.4. Executive Summary. An executive summary, not to exceed one page, shall follow the validation page and precede the body of the Joint DCR.

2.5. Document Body. The body of the Joint DCR shall have the following 5 sections, and shall be no more than 30 pages long. In cases where a limited amount of content is classified at a higher level than the document, an appendix classified at a higher level than the base document may be used to facilitate greater access to the document.

2.5.1. Section 1: Operational Context.

2.5.1.1. The purpose of this section is to provide context for the recommendations addressed by the Joint DCR. This information facilitates the review and validation of the Joint DCR from the standpoint of how the recommendations address or enable solutions to validated capability requirements and contribute to the missions and activities of the joint force.

2.5.1.1.1. Narrative in the operational context section is to be consistent with DoDAF OVs generated during prior analysis, as modified for the scope and purpose of the Joint DCR, including the DoDAF OV-1, OV-2, OV-4, and OV-5a.

2.5.1.1.2. Include the DoDAF OV-1 in this section and, where applicable, ensure high-level intelligence system connectivity and interoperability are accurately and adequately illustrated in the DoDAF OV-1. Do not include other architecture data and associated artifacts/views in the document unless specifically needed for illustration purposes in the body of the Joint DCR. Provide data for the remainder of the required DoDAF OVs in the repository located at the URL specified in the reference section of the document.

2.5.1.2. Describe the range of military operations being addressed and the traceability to relevant parts of the UCP assigned mission, OPLANs/CONPLANs, SSA products. Service and Joint Concepts, CONOPS, and/or other relevant factors to the capability requirements identified in the DCR.

2.5.1.3. If the Joint DCR is a successor document to one or more validated capability requirements documents:

2.5.1.3.1. Cite the validated source document(s) that identified the capability requirements addressed or enabled by the Joint DCR and ensure that any source documents not already present in the KM/DS system are provided to the Joint Staff Gatekeeper for reference purposes.

2.5.1.3.2. From the source document(s), summarize the operational context associated with the validated capability requirements addressed or enabled by the Joint DCR. Ensure any changes to the operational context that have occurred since validation of the capability requirements are addressed. If any changes to the operational context have been made, ensure the DoDAF OVs submitted with the ICD are updated and resubmitted to reflect the applicable changes.

2.5.1.3.3. For Joint DCRs with impact on intelligence equities, ensure any key intelligence support capabilities affected by the changes to DOTmLPF-P are addressed within the operational context.

2.5.1.4. If the Joint DCR is not based on a validated capability requirements document, provide the operational context as outlined for Section 1 of an ICD. If applicable, ensure this section includes reference to relevant JROCMs, CCMD IPLs, joint monthly readiness reviews, quarterly reports to the SecDef, etc., that relate to the change recommendations.

2.5.2. Section 2: Threat Summary.

2.5.2.1. The purpose of this section is to provide context for the capability requirements addressed or enabled by the Joint DCR, to provide appropriate traceability to the DIA- or Service-approved threat products used during refinement of the capability requirements, and to describe updates to the threat products since validation of the capability requirements. When

applicable, this information also enables threat assessment as part of the intelligence certification provided during Joint DCR review and validation, and facilitates rapid review and update of successor documents when applicable threat products are updated.

2.5.2.2. A threat summary is not applicable to all Joint DCRs depending upon the nature of the change recommendations. The Sponsor should coordinate with the proponent for the intelligence certificate, as outlined in Annex G to Appendix G of this enclosure, to determine whether or not a threat summary is required.

2.5.2.2.1. While many Joint DCRs do not require threat assessment or intelligence certification, some may be driven by changes to the threat environment or may propose DOTmLPF-P changes that affect intelligence supportability of fielded capability solutions. In addition, some Joint DCRs may be focused specifically on intelligence activities or fielded capability solutions. In these cases, an intelligence certification generally will be required.

2.5.2.2.2. Sponsors ensure all intelligence support requirements are identified in terms of the broad descriptions of categories described in Annex G to Appendix G of this enclosure, and included in the Joint DCR Operational Context, Capability Discussion, and Implementation Plans sections.

2.5.2.3. If the Joint DCR is a successor document to one or more validated requirement documents:

2.5.2.3.1. Cite the latest DIA- or Service-approved threat products applicable to the capability requirements addressed or enabled by the Joint DCR. Ensure the applicable threat products reflect the most current analysis and findings related to evolving threats.

2.5.2.3.1.1. For Joint DCRs enabling or associated with ACAT ID or ACAT IAM programs, ensure the most current DIA-approved threat products are used to develop the Joint DCR and any associated studies or analysis.

2.5.2.3.1.2. For all other Joint DCRs where threat products are applicable, ensure the most current DIA- or Service-approved threat products are used to develop the Joint DCR and any associated studies or analysis.

2.5.2.3.2. From the source document(s), outline the threat summary(ies) associated with the validated capability requirements addressed or enabled by the Joint DCR.

2.5.2.4. If the Joint DCR is not based on a validated capability requirements document, provide the threat summary as outlined for Section 2 of an ICD, as per Appendix A to this enclosure.

2.5.3. Section 3: Capability Requirements Discussion.

2.5.3.1. The purpose of this section is to identify the validated capability requirements addressed or enabled by the Joint DCR, and to outline the

results of related studies, lessons learned or analysis performed to define the change recommendations.

2.5.3.1.1. Clearly and succinctly describe the capability gap the recommended changes will mitigate or close if implemented.

2.5.3.1.2. Narrative in the capability requirement and capability gap section is to be consistent with DoDAF CVs generated during prior analysis, as modified for the scope and purpose of the Joint DCR, including the DoDAF CV-2, CV-3, and CV-6.

2.5.3.1.3. If the Joint DCR is a successor document to one or more validated capability requirements documents, provide an overview of the validated capability requirements addressed or enabled by the Joint DCR.

2.5.3.1.4. If the Joint DCR is not based on a validated capability requirements document, provide the capability requirement and associated capability gap information outlined for Section 3 of an ICD.

2.5.3.2. Summarize all related analyses, lessons learned and/or studies conducted to develop the change recommendations. Include the alternatives, objective, criteria, assumptions, recommendations, and conclusion. Ensure that final reports, or other resulting products, of studies or analyses not already present in the KM/DS system are uploaded for reference purposes.

2.5.3.3. Ensure any key intelligence support capabilities affected by the changes to DOTmLPF-P are addressed. Ensure the summary highlights any intelligence analyses considered.

2.5.4. Section 4: Change Recommendations.

2.5.4.1. The purpose of this section is to outline recommendations in one or more DOTmLPF-P considerations that provide or enable capability solutions to satisfy validated capability requirements and associated capability gaps. This section also identifies related interdependencies that must be satisfied to provide a successful capability solution.

2.5.4.2. Use this section to describe change recommendations in terms of each applicable joint DOTmLPF-P consideration. See Annex F to Appendix G to this enclosure for more guidance on DOTmLPF-P content.

2.5.4.3. For each change recommendation to a DOTmLPF-P consideration, provide the following:

2.5.4.3.1. Description of the recommended change.

2.5.4.3.2. Changes to tactics, techniques, and procedures (TTPs) and implications on the safe use of the proposed non-materiel solution in the proposed operating environment.

2.5.4.3.3. Forces and systems affected, and any impact on interoperability.

2.5.4.3.4. If a recommendation includes incorporating future technology (materiel component), include a brief discussion of the maturity of critical technology or future systems involved and a risk assessment of the approach.

2.5.4.3.5. Related support that is required to implement recommendations, including, but not limited to, additional research, hardware, DoD manpower, test range time, contractor support, etc.

2.5.4.3.6. Cite any DoD policies or other issues (treaties; protocols; agreements; legal issues; DoD roles, missions, and functions; other U.S. Government agency/department, etc.) that would prevent the effective implementation of the recommended changes and the reason the proposed changes cannot comply with it. Provide proposed changes to the policy or other issue and identify other potential implications from the proposed mitigation.

2.5.4.3.7. If impacted by the recommendations in the Joint DCR, update applicable DoDAF OVs and CVs to reflect how the capability solutions outlined in the Joint DCR address validated capability requirements and close or mitigate associated capability gaps in the capability requirements portfolios without introducing unnecessary redundancy in capability or capacity.

2.5.5. Section 5: Implementation Plans.

2.5.5.1. The purpose of this section is to outline implementation plans for the recommended DOTmLPF-P changes (which will be further refined after validation by the Sponsor or lead organization), and task OPR(s) and affected Joint DOTmLPF-P FPOs.

2.5.5.2. For each change recommendation to a DOTmLPF-P consideration, provide the following:

2.5.5.2.1. Proposed implementation plan, including a Plan of Action and Milestones (POA&M) with start times, major milestones, and completion dates.

2.5.5.2.2. Discussion of relationships between recommendations and associated implementation timing (i.e., a joint organizational change has implications for a personnel change, which influences training plans).

2.5.5.2.3. Ensure fielded or newly introduced key intelligence support capabilities affected by the changes to DOTmLPF-P are identified and adequately addressed in the implementation plan.

2.5.5.2.4. Proposed OPR and rationale. Identify the proposed OPR for each action and provide rationale. Sponsors must attempt to socialize OPR nomination with the affected organizations but may submit a DCR without formal acceptance of the OPR nomination. The validation memorandum will formalize the assignment of the OPR(s). OPRs should be as specific as possible, and when addressing an OPR (or Office of Collateral Responsibility (OCR)) on a joint staff or defense agency, it should be identified down to a department or division level.

2.5.5.2.4.1. If known at the time of staffing, provide organizational POC information for each OPR, including name, organization, office code (if applicable), phone number, and NIPRNET/SIPRNET email addresses. This POC is to be the person responsible for implementing the recommended changes within the OPR. For change recommendations with multiple OPRs (e.g., Services, CCMDs), provide organizational POC information for each applicable OPR.

2.5.5.2.4.2. If POC information for one or more OPRs is not known at the time of staffing, POC information will be determined within 60 days of staffing and provided to the Sponsor of the Joint DCR, the Lead FCB, and affected Joint DOTmLPF-P FPOs. If changes to POC information occur, updated information will be provided to the same recipients.

2.5.5.3. Provide rough-order-of-magnitude total required resources needed to implement the proposed change as shown in Figure B-15, including cost by FY and type of required funding. In cases with funds controlled by different organizations, multiple tables may be used to show changes to funding in each organization.

Required Resource Changes Needed to Implement DOTmLPF-P[1]									
BY$$[2]	**FYxx (Current)**	**FYDP**						**Post-FYDP (FYyy-FYzz)**	**Life Cycle Cost (FYxx-FYzz)**
		FYxx+1	**FYxx+2**	**FYxx+3**	**FYxx+4**	**FYxx+5**	**FYDP Total**		
RDT&E									
Procurement									
MILCON									
O&M									
MILPERS									
Total									

Notes:
[1] Current year is FYxx. First post-FYDP year is FYyy. End of planned capability life, or end of 30-year TOA projection if no planned service life, is FYzz.
[2] All resources normalized to a standard base year reference - BY$$.

Figure B- 15: DCR Summary of Required Resources

2.5.5.3.1. Joint DCRs involve "change recommendations," so cost data represents only new costs or changes to funded efforts. For example, if a recommendation is to change an aspect of joint training, and the change does not require increased resources to cover the total cost of implementing the proposal, including course development, instructor staffing and/or billets, instructor education, facilities, training materials, hardware, and mock-ups, etc., then do not include those resources in this table.

2.5.5.3.2. While cost estimation for non-materiel capability solutions are not bound by the same statutes and policy as materiel capability solutions, Sponsors are encouraged to leverage cost estimation approaches outlined in References [5] and [48]. Ensure that resource estimates have been reviewed by the Sponsor's cost analysis organization to ensure best practices are being

followed. Also, ensure that any final report or other related documentation, not already present in the KM/DS system, is uploaded for reference purposes.

2.6. Appendices. Only the following four appendices are allowed in the document. Additional reference documents or data may be submitted IAW procedures outlined in Enclosure B of this manual.

2.6.1. Appendix A. References. Ahead of other references provided in this appendix, the Architecture must be discoverable and accessible per Appendix H of this enclosure and all architecture data and associated artifacts/views identified in Figure A-4 and, if applicable, Figure B-20 must also be discoverable.

2.6.2. Appendix B. Acronym List. List in alphabetical order, all of the acronyms used in the document.

2.6.3. Appendix C. Glossary. Unless otherwise stated, the terms and definition contained in this glossary are for the purposes of this document only. As the Sponsor develops the document glossary, they may leverage applicable definitions from the DoDAF AV-2. These do not have to be identical, as some terms will only apply to the document or the DoDAF architecture; however, terms that apply to both must be consistent.

2.6.4. Appendix D. (Optional) Classified Appendix. A classified appendix may be used in cases where only a small subset of the document needs to be protected at a higher classification level. If the document is not useful without this appendix, the document is to be classified at a higher level. A classified appendix's content will count toward the document body page limits and will be indexed to align with the baseline document sections. Except where the existence of classified content cannot be acknowledged, each section of the baseline document augmented by the classified appendix will refer the reader to the classified appendix. If used, the appendix shall be provided to the Joint Staff Gatekeeper or J-8, Special Access Program Coordinator (J-8/SAPCOORD) IAW the classification of the appendix.

APPENDIX F TO ENCLOSURE B
JUON/JEON

1. Overview. JUONs, JEONs, and DoD Component UONs are used ONLY when there are urgent requirements for capabilities that do not exist in the joint force, and where the deliberate requirement validation and deliberate acquisition processes, or other means such as the GFM process, JMVP, etc., are not practical for satisfying the capability requirements in the operational timelines. JUONs and JEONs support urgent and emergent capabilities associated with on-going and anticipated contingency operations as outlined in Appendix B of Enclosure A; and as such, Sponsors should field an initial capability solution in less than 2 years.

1.1. Purpose. The purpose of JUONs, JEONs, and DoD Component UONs is to facilitate rapid identification, prioritization, validation, documentation, and communication of urgent or emergent capability requirements and associated capability gaps that represent significant risk to mission success or safety of forces. These documents serve as the basis for expedited validation by the validation authority identified in Enclosure A of this manual. The acquisition of materiel capability solutions in response to validated capability requirements is addressed IAW Reference [26].

1.1.1. DoD Component UONs are applicable to only one DoD Component guided by ongoing or anticipated contingency operations. Component UONs are submitted, staffed, and validated IAW References [17], [20], [21], [22], [23], [24], and [25]. Within 14 days of validation, the Sponsor shall provide DoD Component UONs to the Joint Staff Gatekeeper for information and visibility in the capability requirements portfolios.

1.1.2. JUONs and JEONs affect two or more DoD Components. JUONs and JEONs are guided by ongoing and anticipated contingency operations submitted by Combatant Commanders (CCMDs) or CJCS/VCJCS and reviewed and validated IAW Enclosure A of this manual.

1.1.2.1. JUONs are staffed IAW this manual and validated by the J-8/DDRCD.

1.1.2.2. JEONs are staffed IAW this manual and validated by the JCB or JROC.

1.1.3. JUONs and JEONs are primarily submitted by CCDRs. CCDRs will also review, validate and adjudicate UON requests between Components to further expedite capabilities already in existing use.

1.1.4. While JUONs and JEONs are primarily submitted by the CCMDs, the CJCS/VCJCS may generate a JUON or JEON directly in support of CJCS or VCJCS responsibilities, or to facilitate timely validation of urgent or emergent needs identified by multiple CCMDs or DoD Components.

1.1.5. DoD Components that require a capability that is resident in the inventory of another Service may coordinate with the cognizant organizations for potential use of the processes in References [17], [20], [21], [22], [23], [24], and [25].

1.2. Applicability.

1.2.1. JUONs, JEONs, and DoD Component UONs are appropriate for the following:

1.2.1.1. Capability requirements that can have an initial capability solution fielded within 2 years.

1.2.1.2. JUONs. Capabilities that are driven by ongoing contingency operations that are necessary to prevent loss of life or critical mission failure that require out-of-cycle funding to initiate program execution.

1.2.1.3. JEONs. Capabilities that are driven by anticipated contingency operations necessary to prevent loss of life or prevent critical mission failure, and where out-of-cycle funding is required to initiate program execution.

1.2.2. JUONs, JEONs, and DoD Component UONs are not appropriate for the following:

1.2.2.1. Capability requirements that cannot provide an initial capability solution fielded within 2 years.

1.2.2.2. Capability requirements not associated with ongoing or anticipated contingency operation and not directly related to the prevention of loss of life or not considered to cause critical mission failure if the capability gap is not filled in an expeditious manner.

1.3. Proponent. The proponent for this appendix is the J-8/JCD. For questions, contact J-8/JCD at (703) 695-2705.

2. Format. JUON and JEON format is addressed in this section. See References [17], [20], [21], [22], [23], [24], and [25] for format of DoD Component UONs.

2.1. Cover Page. JUONs and JEONs do not require a cover page.

2.2. Validation Page. JUONs and JEONs do not require a validation page.

2.3. Executive Summary. JUONs and JEONs do not require an executive summary.

2.4. Document body. JUONs and JEONs will be in memo format and generally not to exceed three pages.

2.4.1. Section 1. Administrative Data.

2.4.1.1. Title. (Unclassified version).

2.4.1.2. Submitted by. (e.g., USCENTCOM).

2.4.1.3. Authorized by. Release authority's name, rank, and title. New JUONs and JEONs, and modifications to the capability requirements in validated JUONs and JEONs, must be endorsed by the Combatant Commander, Deputy Commander, or Chief of Staff. The CCMD J-8 may endorse administrative modifications to validated JUONs or JEONs.

2.4.1.4. Primary and secondary POCs for the document Sponsor: Include name, title/rank, phone, and both NIPRNET and SIPRNET email addresses. POCs must have completed the appropriate level of RMCT IAW Enclosure A of this manual.

2.4.1.5. Date submitted by the CCMD.

2.4.2. Section 2: Operational Context and Threat Analysis. What is the target, threat, or operational deficiency? What cannot be done without a new or improved capability solution? Identify where the operational deficiency exists, describing the mission deficiency or capability gap. Describe in detail the nature of the urgency and the operational impact, if not immediately resolved, in terms of critical mission failure or loss of life. Provide a CONOPS for which the capabilities requested in the JUON or JEON contribute, including information regarding the coalition environment within which the capability solution will need to operate.

2.4.3. Section 3: Required Capability. Describe what capabilities are required, as opposed to capability solutions that will be addressed later, and whether they support a discrete operation, must be sustained for an extended period, or must be sustained until the end of the conflict. The capability requirements must be specifically articulated in light of the operational context and cannot involve broad/unquantified requests. Include threshold joint performance requirements for the relevant key attributes. If these attributes are designated as JPRs, they will automatically be upgraded to KPPs. The threshold joint performance requirements are the parameters necessary to prevent loss of life and/or critical mission failure. This description must also specify the latest acceptable date to address the capability requirements and associated capability gaps.

2.4.4. Section 4: Flexibility. In the event of technological or other challenges, indicate whether receiving a partial capability solution on schedule is preferred to a delayed capability solution that satisfies a greater portion of the capability requirement. Estimate acceptable percentages of reduced performance and/or acceptable delay timeframes.

2.4.5. Section 5: Potential Non-Materiel Capability Solutions. Describe any non-materiel options and alternatives that were considered, or which provide partial mitigation of the capability requirement.

2.4.6. Section 6: Potential Materiel Capability Solutions. If known, identify and discuss viable capability solutions – including those from other DoD Component, other U.S. Government agency/department, or allied/partner nation sources in addition to commercial sources – that could improve

operational capabilities or system performance. Discuss any impacts to safety, survivability, personnel, training, logistics, communications, etc. If applicable, discuss any market survey or similar related information developed by the document Sponsor or during the validation process. If market research details are available, provide along with the JUON or JEON to facilitate reuse during rapid acquisition activities. Unless granted an exemption to ISP requirements IAW Reference [10], JUON, JEON, and DoD Component UON solutions must comply with the net-ready certification guide as outlined in Annex A to Appendix G to this enclosure.

2.4.7. Section 7: Required Quantities. For materiel capability solutions, identify required quantities and distribution among applicable DoD Components.

2.4.7.1. Total quantities must include both the required operational inventory, as well as required quantities for training, spares, scheduled repair/overhaul pipeline, and anticipated attrition over the projected lifecycle, so that the required operational inventory is maintained.

2.4.7.2. Changes to quantities intended solely to accommodate unexpected attrition, or expenditure in the case of munitions, and maintain the required operational inventory, do not require revalidation of the capability requirements.

2.4.7.3. Changes to production quantities, or absence of changes to production quantities when consumption or attrition rates change from original planning which result in changes to the operational inventory, will require revalidation of required operational inventory quantities and/or acceptance of the altered operational risk.

2.4.8. Section 8: Limitations. Identify any known limitations that could inhibit satisfying the need, such as arms control treaties, logistics support, transportation, manpower, training, existing regulations, policies or guidance, or non-military barriers.

APPENDIX G TO ENCLOSURE B
DEVELOPMENT OF PERFORMANCE ATTRIBUTES

1. Overview.

1.1. Purpose. The purpose of this appendix is to specify the performance attributes for capability development. It defines KPPs, KSAs, and APAs.

1.2. Applicability. The development of performance attributes are applicable to all CDDs and IS-CDDs as specified in Appendix C and Appendix D of this enclosure. The annexes to this appendix provide guidance on required performance attributes.

1.3. Proponent. The proponent for this appendix is J-8/JCD; the annexes to this appendix specify proponents for certifications and endorsements. For questions, contact J-8/JCD at (703) 695-2705.

2. Performance Attributes. Performance attributes are characteristics or inherent parts of a system required for the system to achieve satisfactory performance. Sponsors must establish performance attributes (KPPs, KSAs, and APAs) which are technically achievable, quantifiable, measurable, testable, unambiguous, supported by documented trade-off analysis, and defined in a manner that supports efficient and effective T&E. The number of performance attributes specified by a Sponsor should be kept to a minimum to maintain program flexibility. It is important to note that based on recent FY17 NDAA guidance there is a distinction that will be made as to whether or not each of the performance attributes (KPP, KSA, or APA) listed in the capability requirements documents have joint equity that will be designated by the Joint Staff Gatekeeper as JPRs IAW Reference [2].

2.1. KPPs. These are the performance attributes of a system considered critical or essential to the development of an effective military capability. Failure of a system to meet a validated KPP threshold value triggers a review by the validation authority and evaluation of operational risk and/or military utility of the associated system(s). The review may result in validation of an updated KPP threshold value, modification of production increments, or recommendation for program cancellation.

2.2. KSAs. Performance attributes of a system considered important to achieving a balanced solution/approach to a system, but not critical enough to be designated a KPP.

2.3. APAs. Performance attributes of a system not important enough to be considered KPPs or KSAs, but still appropriate including in the CDD.

2.4. Sponsors should consider the appropriate tradespace between threshold and objective values in the development of their performance attributes. Ensure tradespace is sufficient to allow for new technologies, evolving threats, and interoperability needs.

2.5. Post-validation Change Authority. Post-validation change authority for KPPs, KSAs, APAs, and document content affecting certifications and endorsements is determined by the JSD level and whether or not the attribute is designated as a JPR.

3. Mandatory Performance Attributes. In addition to KPPs, KSAs, and APAs essential to the capability solution being developed, Sponsors shall address the following four Mandatory KPPs as well as the Net-Ready Performance Attribute. Force Protection, System Survivability, Sustainment, and Energy attributes will remain Mandatory KPPs IAW the applicable provisions of federal law under Title 10 U.S.C.

3.1. Force Protection (FP) KPP (Mandatory KPP). The FP KPP is intended to ensure protection of occupants, users, or other personnel who may be adversely affected by the system or threats to the system. Additional guidance is provided in Annex B to this appendix.

3.2. System Survivability (SS) KPP (Mandatory KPP). The SS KPP is intended to promote the development of critical warfighter capabilities that can survive kinetic (i.e., traditional, non-traditional, and CBRN (including EMP)) and non-kinetic (cyber and EMS)) threats across domains and applicable environments including space. Additional guidance is provided in Annex C to this appendix.

3.3. Sustainment KPP (Mandatory KPP). The Sustainment KPP is intended to ensure an adequate quantity of the capability solution will be ready for tasking to support operational missions. Additional guidance is provided in Annex D to this appendix and in Reference [51].

3.4. Energy KPP (Mandatory KPP). The Energy KPP is intended to ensure combat capability of the force by balancing the energy performance of systems and the provisioning of energy to sustain systems/forces required by the operational commander under applicable threat environments. Additional guidance is provided in Annex E to this appendix.

3.5. Net-Ready Performance Attribute. The net-ready performance attribute ensures interoperability between individually developed and fielded capability solutions. Additional guidance is provided in Annex A of this appendix.

4. Required Certification or Endorsement. Prior to validation of CDDs and IS-CDDs, assessing organizations will provide the Lead FCB (for all JPR-designated performance attributes) with a certification or endorsement memorandum, concurrence that the certification or endorsement is not required, or changes the Sponsor must make in order to receive the certification or endorsement. Only required attributes considered JPRs will need a Joint Staff certification and/or endorsement. All other attributes will be delegated to the appropriate independent validation authority to certify or endorse.

4.1. Waivers. The Sponsor must address all required certifications and endorsements unless specifically waived prior to validation of a capability

requirements document. In cases where a Sponsor proposes that the required attribute is not appropriate to the operational context of a capability solution, the Sponsor shall justify why that required performance attribute is not appropriate. See the individual annexes in this appendix for information about certifying and endorsing organizations and the means of requesting a waiver or exemption to required performance attributes.

4.1.1. To ensure efficient staffing, Sponsors are encouraged to seek approval from the appropriate certifying or endorsing official for any performance attribute they believe does not have joint equity or does not apply prior to submitting a capability requirements document.

4.1.2. In cases where a predecessor document did not include a Mandatory KPP because it was not defined or was not mandated in an earlier version of JCIDS, the Sponsor will either include the Mandatory KPP in the successor document or work with the appropriate certifying or endorsing organization to ensure the intent of the Mandatory KPP is otherwise captured in the document.

5. Thresholds, Objectives, and Tradespace. Sponsors shall express performance attributes using a threshold/objective format. They are chosen to be technically achievable, quantifiable, measurable, testable, unambiguous, supported by documented trade-off analysis, and defined in a manner that supports efficient and effective T&E. IAW Reference [5], Sponsors include KPPs verbatim in the acquisition program baseline.

5.1. Thresholds. Performance below the threshold value is not operationally effective or suitable or may not provide any improvement over current capabilities. Context must be provided to articulate what operational impact or risk is unacceptable if the performance were to fall below the threshold value. The threshold value for a performance attribute must also be considered achievable within the projected lifecycle cost, schedule, and technology at low-to-moderate risk.

5.2. Objectives. The objective values are applicable when a higher level of performance represents significant increase in operational utility. Context must be provided to articulate what operational impact or risk is further mitigated if the performance were to reach the objective value. If applicable, the objective value is the desired operational goal achievable, but at higher risk in lifecycle cost, schedule, and technology. Performance above the objective value does not justify additional expense.

5.3. Tradespace. The difference between threshold and objective values sets the trade space for balancing multiple performance attributes while remaining above the threshold values. Advances in technology, evolving threats, or changes in approved Service and Joint Concepts may result in proposals to change threshold and objective values in future increments of a capability solution. Ensure tradespace is sufficient to allow the Sponsor to pursue increased capability in the future to meet the evolving threat without having to revalidate the requirement.

6. Development of Performance Attributes. The Sponsor designates appropriate performance attributes dependent upon the nature of the system and its intended capabilities. For documents with JSDs of JROC Interest or JCB Interest, the JCB or JROC may designate additional performance attributes as JPRs, or modify threshold or objective values, based on the recommendation of the FCBs.

6.1. Initial Questions. The following questions should be answered in the affirmative before a performance attribute is selected for the increment being defined:

6.1.1. Is the performance attribute traceable and does it satisfy one or more operational attributes of joint military capability requirements validated in an ICD?

6.1.2. Does the threshold value of the performance attribute contribute to significant improvement in warfighting capabilities, operational effectiveness, and/or operational suitability, where an inability to meet the threshold value should call into question the continued value of the program?

6.1.3. Are the necessary combinations of performance attributes and their threshold/objective values, identified in a manner that allows for assessment of their ability to achieve mission success in the operational context? Are the combinations of performance attributes consistent with the CONOPS and/or the Operational Mode Summary/Mission Profile (OMS/MP) documentation? For example:

6.1.3.1. If an individual system includes performance attributes such as range, payload, and loiter time, different missions intended for the system may require the performance attributes in different combinations.

6.1.3.2. Meeting each performance attribute in isolation might not provide any mission value and not allow operations consistent with the OMS/MP, i.e., meeting required range without any munitions or loiter time, meeting required payload without any range or loiter time, or meeting required loiter time without any range or payload.

6.1.3.3. Meeting each performance attribute in combination, using the required maximum values for any one mission, but without the context of the individual missions may allow operations consistent with the OMS/MP, but lead to an unreasonably expensive or unachievable capability solution, i.e., combining the required payload for short heavy lift missions with the required range for an empty ferry flight mission with the required loiter time for a lightly armed surveillance mission does not properly reflect the capability requirements of the system nor the set of conditions against which it should be tested.

6.1.4. Are the recommended threshold and objective values of the performance attribute reflective of reasonable operational risks, applicable technology

maturity, timeframe the required capability is needed, and supported by analysis?

6.1.5. When justifiable in terms of warfighter benefit, is their adequate trade space between the threshold and objective values of each of the performance attributes to accommodate future changes caused by evolving technologies, threats and interoperability needs so as to not require revalidation?

6.1.6. Is the threshold value of the performance attribute achievable and affordable, considering projected lifecycle costs and limitation of Service and DoD projected TOA over the FYDP and future year projections?

6.2. T&E Considerations.

6.2.1. Very tightly specified performance attributes are resource intensive to test with confidence. When such specificity is needed, the Sponsor must consider the T&E resource implications of requiring capabilities to perform to such low tolerances.

6.2.2. Avoid specifying all-inclusive values for parameters, such as all/never, 0/100 percent, all-sensors, all weather, all/none of the time, no/every situation, etc. These kinds of values generally are impossible to achieve and require an infinite amount of testing to prove statistically.

6.2.3. Other choices made when specifying performance attributes may require higher or lower T&E resources. For example, probability metrics are expensive to test because they require large sample sizes to gain statistical confidence in the results. However, if meaningful continuous metrics that relate to the probability metrics can be derived, T&E resources may be significantly reduced.

6.2.4. Interactions between Sponsors and the T&E community during development of performance attributes can help identify more testable alternatives.

6.3. Example development methodology. The following set of steps is one methodology for developing performance attributes:

6.3.1. List capability requirements for each mission or function as described in the proposed CDD. This review should include all capability requirements that the system described in the CDD is projected to meet, including those related to other systems in an FoS or SoS context. It shall also include all relevant performance metrics identified in ICDs for which the CDD is providing a capability.

6.3.2. For each critical mission or function, build at least one measurable and unambiguous performance attribute, without yet designating it as a KPP, KSA, or APA, using the list from the previous step as a starting point.

6.3.3. Determine the performance attributes most critical or essential to the system(s) and designate them as KPPs. Other important performance attributes can be assigned as KSAs or APAs. Note that a KPP need not be

created for all missions and functions for the system(s), as a KSA or APA may be used without an overarching KPP. In contrast, certain missions and functions may require two or more KPPs.

6.3.4. Document how the performance attributes are traceable to the operational attributes and associated values of the capability requirements identified in the ICDs and associated DoDAF CV-3 or other predecessor documents. This ensures that performance attributes support mission outcomes and other associated desired effects.

6.3.5. Set threshold and objective values for performance attributes.

6.3.5.1. Threshold values are to be based on the minimum required performance needed to achieve the required operational effect, while being achievable through the current state of technology at an affordable system lifecycle cost. Technology achievability is based on the technology behind delivery of the performance having achieved technology maturation sufficient for Milestone B; or system or sub-system performance being on track to achieve TRL 6 or greater prior to Milestone B.

6.3.5.2. Objective values are to be defined where an increased level of performance delivers significant increased operational effect, or decreased operational risk, if it can be delivered at an affordable system lifecycle cost. Not every performance attribute must have an objective value that differs from the threshold value but providing trade space between threshold and objective values allows the Sponsor greater flexibility before having to pursue revalidation of changes to requirements documents.

6.4. Refinement of threshold and objective values. Threshold and objective values of a performance attribute may change between the Sponsor Draft CDD prior to Milestone A to the validated CDD prior to Milestone B to follow on milestone decisions. The threshold and objective values specified for the performance attributes in the Sponsor Draft CDD are used to guide the acquisition community during TMRR as well as used in the validated CDD to guide acquisition community during EMD.

6.4.1. During TMRR, the threshold and objective values should drive exploration of technologies and risk reduction activities. It is likely the performance attribute threshold and objective values may change during this phase.

6.4.2. During EMD, tradeoffs are made between the threshold and objective values to optimize performance given the available technology for the increment and the competing demands introduced by combining subsystems into the overall system.

6.4.3. A deeper analysis of cost-capability trade-offs at and around threshold and objective values may be beneficial to decision makers, by exploring incremental return on investment where certain performance attributes might

be insensitive to small deviation at great advantage in lifecycle cost, performance, schedule, and quantity reviews.

6.4.4. After the Critical Design Review (CDR), these tradeoff decisions are essentially completed and a more precise determination of acceptable performance can be stated in an update to the CDD if required.

6.4.5. Performance attribute development over time.

6.4.5.1. Figure B-16(a) shows an individual performance attribute of a system with threshold and objective values (1 and 10, respectively) as specified in the Sponsor's Draft CDD prior to Milestone A.

6.4.5.2. With further refinement and as determined during the TMRR phase of acquisition and presented in the CDD submitted for validation, the objective values may decrease due to technology limitation, as shown in Figure B-16(b)

6.4.5.3. In cases where the threshold values fall below those identified in the original CDD, the Sponsor must return to the validation authority to revalidate the proposed performance attributes. They must justify why the decrease in threshold values still provides military value to the joint warfighter and the reason for the decrease, which may include resource, technology, or other limitations. Figure B-16(c) depicts this situation.

6.4.5.4. During EMD, optimum performance values may be identified based on lifecycle cost, performance, or other considerations, as shown in Figure B-16(d).

6.4.5.5. Further design tradeoffs among the collective performance attributes may necessitate settling for design performance values higher or lower than the optimum values for the individual performance attributes. Figure B-16(e) shows an example in which optimum performance was traded off because of other considerations, resulting in reduced performance within this performance attribute.

6.4.5.6. If required, the updated CDD prior to Milestone C may include threshold and objective values that are revised versions of the values documented in the CDD. Figure B-16(f) shows an example of the revised performance attributes. Note that these values are not necessarily bounded between the original threshold and objective values.

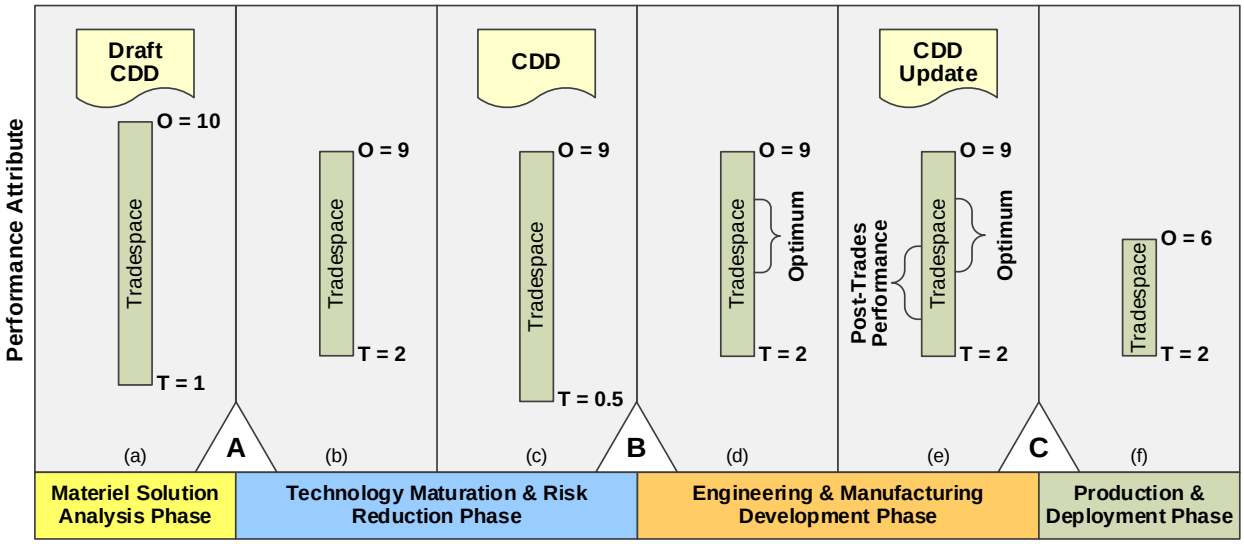

Figure B- 16: Performance Attribute Evolution

6.4.5.7. Each threshold value is to be assessed against knowledge gained during the TMRR and EMD phase of acquisition. Performance attribute (KPP, KSA, and APA) threshold values in the updated CDDs generally will denote equal or increased performance over the initial CDD threshold values. In cases where performance attribute threshold values are reduced in an updated CDD, the following issues must be addressed in the CDD:

6.4.5.7.1. What are the impacts to military utility and operational risk from performance below the original threshold value?

6.4.5.7.2. If the new capability solution is intended to replace a fielded capability solution, will it still provide more overall military utility than the fielded capability solution?

6.4.5.7.3. Is the reduced performance of this capability solution still a good way to address the capability requirement and close or mitigate the associated capability gap, or should a different materiel or non-materiel alternative approach be considered?

6.4.5.7.4. Is the reduced performance of the capability solution worth the additional required investments needed to continue the program to completion?

6.4.5.7.5. What level of increased investment might be required to maintain the original threshold performance? If pursued, where will the additional funds come from while remaining below projected TOA, and what operational risks are involved with the source of the additional funds?

6.4.5.8. For an early increment in an incremental approach to acquisition, the production objective value for the increment could be less than the development threshold value, with later increments providing performance at or above the threshold. In that case, plans must be in place to upgrade early increments to meet threshold values, or to use early increments to support less

demanding missions, and later increments to support missions that are more demanding.

6.4.5.9. Trade space between threshold and objective values of performance attributes may also be exercised by Sponsors to support later upgrades of a capability solution without revalidation of a capability requirements document, as long as there are no changes to operational context or threats that would otherwise require revalidation.

7. Requesting Relief from a Validated Performance Attribute. JROC encourages the Sponsor, in coordination with the MDA, to request requirements relief from the validation authority when cost-benefit analyses indicate validated performance attributes may drive costs out of proportion with the capability delivered to the operational user.

7.1. Gatekeeper routing. All requests for relief on KPPs designated as JPRs are routed through the Joint Staff Gatekeeper to the appropriate FCB and other stakeholder organizations.

7.2. Changing context over time. While the performance attributes documented and validated in capability requirements documents represent the validation authority's best military advice at an instant in time, knowledge gained through acquisition activities, changes to strategic guidance, external threats, mission requirements, or budgetary realities may make relief from validated performance attributes appropriate.

7.3. Budgetary considerations. While there are no limitations for requesting requirements relief, relief from KPPs designated as JPRs should be considered especially appropriate in cases where significant cost savings may be achieved with marginal impact on operational capability, i.e., spending 15 percent of a program's budget to get the last 3 percent of a designated threshold if the operational risk involved with a reduced threshold is minimal.

ANNEX A TO APPENDIX G TO ENCLOSURE B
NET-READY GUIDE

1. Overview.

1.1. Purpose. The net-ready content within the Joint Interoperability Section of the CDD and IS-CDD ensures interoperability between individually developed and fielded capability solutions. As part of the statutory duties of the JROC, it must ensure DoD Components develop, acquire, test, deploy, and maintain IS that:

1.1.1. Meet the essential operational needs of U.S. forces.

1.1.2. Are interoperable and supportable with fielded, developing, and proposed (pre-Milestone A) IS through architecture, standards, defined interfaces, modular design, and reuse of fielded IS solutions.

1.1.3. Use architecture data and associated artifacts/views to develop the net-ready content that is:

1.1.3.1. Certified in capability requirements documents IAW this manual.

1.1.3.2. Reviewed in Information Support Plans (ISPs) IAW Reference [10].

1.1.4. Are supportable over the DoD Information Network (DoDIN) IAW Reference [52] and as defined in Reference [53].

1.1.5. Are interoperable with host nation, multinational coalition, and federal, state, local, and tribal agency partners.

1.1.6. Provide global authentication, access control, and enterprise directory services; provide information and services to the edge; use joint information environment operational reference architecture (JIE ORA); provide unity of command; and comply with common policies and standards IAW References [54] and [55].

1.1.7. Leverage emerging capability-based references and methods, including JCAs as described in this manual and Reference [56], Joint Mission Threads (JMTs) as described in Reference [57], and the Joint Common System/Service Function List (JCSFL) as described in Reference [58].

1.1.8. Comply with spectrum and E3 control requirements throughout the capability solution's lifecycle.

1.1.9. CCMDs, Services, and other DoD Agencies ensure capability solutions are aligned with and interoperable during the development cycle.

1.1.10. Comply with DoD Interoperability policy and instruction IAW Reference [10].

1.1.11. Comply with DoD Cybersecurity policy IAW References [59], [60], [61], and [62]

1.2. Applicability.

1.2.1. Capability Documents. The net-ready content in Section 7, the Joint Interoperability Section, is applicable to all CDDs and IS-CDDs.

1.2.2. IS. All IS will follow the net-ready development process IAW this guide and Reference [42], [59], [63], and [64].

1.2.2.1. This applies to all IS acquired, procured, or operated by any DoD Component including, but not limited to:

1.2.2.1.1. National Security Systems (NSS).

1.2.2.1.2. Automated IS (AIS) acquisition programs.

1.2.2.1.3. IS initiatives, IS services, software.

1.2.2.1.4. Electronic warfare devices.

1.2.2.1.5. DBS.

1.2.2.1.6. Prototypes as described in Reference [5].

1.2.2.1.7. COTS, Leased, and GOTS.

1.2.2.1.8. JCTD.

1.2.2.1.9. Coalition Warrior Interoperability Demonstration.

1.2.2.1.10. CCMD Initiatives Fund (CCIF).

1.2.2.2. It does not apply to non-DoDIN IT, including self-contained or embedded IT that is not, and will not be, connected to the enterprise network as defined by Reference [52].

1.2.2.3. The net-ready content identified in Section 7 of the CDD will be used in the ISP to identify required support needed from external IS. When identified as applicable for a given capability requirement, the net-ready content is required for all program increments.

1.2.3. Applicability of net-ready content is not required prior to validation of JUONs, JEONs, and DoD Component UONs. However, net-ready must be considered in the following instances listed below:

1.2.3.1. IT fielded under JUONs, JEONs, and DoD Component UONs, and proposed for transition to enduring use must comply with the net-ready content as part of transition IAW this enclosure, and net-ready certification IAW Reference [10], including:

1.2.3.2. As data from the net-ready content is used in part to support approval of ISPs, the need for a net-ready content may be waived if an exemption to the ISP is approved IAW Reference [10], including:

1.2.3.2.1. The DoD Component places the IT using this exemption on the Operating At Risk List (OARL) before network connection, and

1.2.3.2.2. The individual enclave owner(s) determine whether to allow the IT listed on the OARL to connect.

1.2.3.3. IT fielded under JUONs, JEONs, and DoD Component UONs meet the threshold for MDAP do not qualify for this exemption.

1.3. Proponent: The proponent for net-ready is the C4/Cyber FCB. For questions, please contact the C4/Cyber FCB at (703) 692-6529.

2. Net-Ready Content Guide.

2.1. Net-Ready Performance Attributes. Net-Ready performance attributes determine criteria for interoperability, and operationally effective end-to-end information exchanges which are traceable to their associated operational context, and are technically achievable, quantifiable, measurable, testable, unambiguous, supported by documented trade-off analysis, and defined in a manner that supports efficient and effective T&E.

2.1.1. The net-ready content identifies operational, communications and computers requirements in terms of threshold and objective values for MOEs and MOPs. The net-ready content covers all communication, computing, EM spectrum, and E3 control requirements involving information elements among producer, sender, receiver, and consumer. Information elements include the information, product, and service exchanges. These exchanges enable successful completion of the warfighter mission or joint business processes. Additionally, net-ready content and the three attributes listed below may relate to the intelligence interoperability requirements (found in the Intelligence Supportability Guide under Annex G to Appendix G to this enclosure). Sponsors should ensure consistency between net-ready content and any intelligence interoperability requirements identified in the document.

2.1.2. The net-ready content includes three attributes derived through a three-step process of mission analysis, information analysis, and systems engineering and architecture. These attributes are then documented in solution architectures developed according to the current DoDAF standard in Reference [6].

2.1.2.1. Attribute 1. Support to military operations. This attribute specifies which military operations (e.g., missions or mission threads), as well as operational tasks, a system supports. Threshold and objective values of MOEs are used to measure mission success and are to the conditions under which a mission will be executed. Threshold and objective values of MOPs are used to measure task performance. The conditions define the environment under which the tasks are performed. Values must be presented in numerical form whenever possible. Since the net-ready content focuses on exchanging information, products, or services with external IS, these tasks may be communications and computers operational tasks. Operational tasks are

related to communications and computers if they produce information, products, or services for or consume information, products, or services from external IS (including storing information on external IS).

2.1.2.2. Attribute 2. Entered and be managed on the network. This attribute should specify which networks the system must connect to in order to support its military operations. Unlike the Support to Military Operations attribute, this net-ready performance attribute does not have a standardized framework of terminology and metrics. Therefore, programs should ask a series of questions to develop the derived requirements of this attribute. These questions should be in the context of the missions and tasks a program supports and include:

2.1.2.2.1. What types of networks will the system connect to? (This includes more than just IP networks.)

2.1.2.2.2. What metrics do the required networks use to measure network entrance and management performance? This should include metrics used to measure the time from system start up to when the system has connected to the network and is supporting military operations.

2.1.2.2.3. Who will manage the system as it connects to various networks?

2.1.2.2.4. How will the system be managed? Will management be distributed, centralized, local, remote, etc.?

2.1.2.2.5. What configuration parameters does the network have?

2.1.2.3. Attribute 3. Exchange information. This attribute specifies the information elements produced and consumed by each mission and net-ready operational task identified above. It identifies information elements the IS produces, sends, or makes available to external or joint interfaces and information elements the IS receives from external or joint interfaces (since net-ready content focuses on interactions with external systems, e.g., potential interactions with allied/partner nations and other U.S. Government systems). For each information element, MOPs are used to measure the information element's production or consumption effectiveness. The net-ready MOPs also should describe the information elements' continuity, survivability, interoperability, security, and operational effectiveness and how unanticipated uses could be affected.

2.2. Net-Ready Content Functions. The net-ready content is used to address:

2.2.1. Requirements. Evaluate interoperability and communications and computers requirements for the system.

2.2.2. Information Exchanges. Verify IS supports operationally effective producer to consumer joint information exchanges according to the validated capability requirements, applicable reference models, and reference architectures.

2.2.3. MOEs and MOPs. Provide MOEs and MOPs to evaluate the IS's ability to meet the initial objective values for requirements validated under an ICD, threshold and objective values for requirements validated under a CDD, or initial minimum values for requirements validated under an IS-ICD or IS-CDD.

2.2.4. Interoperability Issues. To enable assessment of capabilities and systems, architectures must align with and use the JCSFL. The architecture should also align, if applicable, with the DoD IEA existing JMTs. These alignments enable identification of potential interoperability disconnects with interdependent systems or services as well as detailed information exchange and information sharing strategies.

2.2.5. Compliance. Determine whether IS complies with network operations (NETOPS) for the DoDIN direction, DoDIN goals and characteristics, and is integrated into system development, IAW Reference [54].

2.2.6. Spectrum Requirements. To obtain a net-ready certification, all IS must comply with spectrum management and E3 direction. The spectrum requirements process includes joint, DoD, national, and international policies and procedures for the management and use of the EM spectrum. Details on compliance are available at the URL in Reference [42].

2.2.7. EMSO Requirements. To support EMSO data exchange requirements, all spectrum dependent systems (transmitters, receivers, etc.) will provide data to characterize the electromagnetic operating environment (EME). Details on compliance are available in Reference [43]. In order to guide development and integration of multi-INT and electronic warfare sensors to achieve aperture-agnostic geolocation, targeting, identification and assessment, multi-INT cooperative operations will be assessed and validate through the JCIDS process. Ensure that All Domain-Overhead Cooperative Operations (AOCO) activities trace to valid joint capability requirements. Details on compliance are available in Reference [65].

2.3. Net-Ready Content Development. Unless defined as non-DoDIN IT by Reference [52], all IS require the net-ready content that specifies interoperability requirements which are traceable to their associated operational context and are technically achievable, quantifiable, measurable, testable, unambiguous, supported by documented trade-off analysis, and defined in a manner that supports efficient and effective T&E. Interoperability requirements include both the technical information exchanges and the operational effectiveness of those exchanges.

2.3.1. Primary Questions. Net-Ready content development uses a three-step question/answer process to develop threshold/objective values.

2.3.1.1. What military operations are being supported?

2.3.1.2. What networks are being used?

2.3.1.3. What information is to be exchanged between joint interfaces/joint entities?

2.3.1.4. What is the required security needed to protect the information used or produced by the system/capability?

2.3.1.5. Figure B-17 depicts this three-step process. Additional guidance on net-ready content development is available at Reference [42].

NR Development Step	NR Performance Attribute	Attribute Details	Measures	Sample Data Sources
Mission Analysis	Support to Military Operations	Mission Statement	Overall real-world military mission of the system	Executive Summary, CONOPS, AV-1
		Mission Activity	Joint Mission Activity	OV-5a/b or Document
		Measure	Measure to determine the success of the Joint Mission Activity supporting the military operation	SV-6/SvcV-6 or SV=7, or Document
		Conditions	Conditions under which the military operations must be executed	Document
		Network	Network the system must connect to in order to support its military operations	SV-1/SV-2 or Document
Information Analysis	Entered and Be Managed on the Network	Measure	Time to connect to and/or how system is managed on the network	OV-3, SV-6/SvcV-6 or SV-7
		Network	Network the system must connect to in order to support its military operations	SV-1/SV-2 or Document
		Measure	Time to connect to and/or how system is managed on the network	OV-3, SV-6/SvcV-6 or SV-7
		Conditions	Conditions under which the military operations must be executed	Document
		Information Element	Type/kind of data being exchanged between Joint entities	OV-3, SV-6/SvcV-6 or SV-7
	Exchange Information	Measure	Performance attribute/ measure of success per Joint information exchange	OV-3, SV-6/SvcV-6 or SV-7
		Conditions	Conditions under which the military operations must be executed	Document
		Information Element	Type/kind of data being exchanged between Joint entities	OV-3, SV-6/SvcV-6 or SV-7
		Measure	Performance attribute/ measure of success per Joint information exchange	OV-3, SV-6/SvcV-6 or SV-7
		Conditions	Conditions under which the military operations must be executed	Document

NR Development Step	NR Performance Attribute	Attribute Details	Measures	Sample Data Sources
		Ensures that IS satisfies the attribute requirements Accessed from the enterprise Which services do military operations require?	Provides traceability from the IS Measure to the derived operational requirements Measures, Sample Architecture Data Sources	OVs, SVs, StdV-1/ StdV-2, and/or SvcVs
Systems Engineering and Architecture	Supports all three attributes			

Figure B- 17: Net-Ready Attribute Sources Table

2.4. Net-Ready Architecture Development Methodology. Architecture development enables development of the net-ready. Architecture-based solutions, developed through a strict verification and validation process, are fundamental for improved interoperability, better information sharing, stricter compliance, and leaner processes. They also feed into system engineering processes and ultimately result in reduced lifecycle costs and more effective mission accomplishment. Reference [6] describes the six-step architecture development process for DoD that is shown in Figure B-18. The six-step architecture development process supports the three-steps of net-ready development described in this manual. Solution architectures, conforming to the current DoDAF standard, are developed, registered, and used as tools to improve joint operational processes, infrastructure, and solutions and to promote common vocabulary, reuse, and integration. Additionally, architecture development enables compliance with the net-ready certification requirements. Figure B-18 shows the net-ready development steps in relation to the JCIDS and acquisition processes.

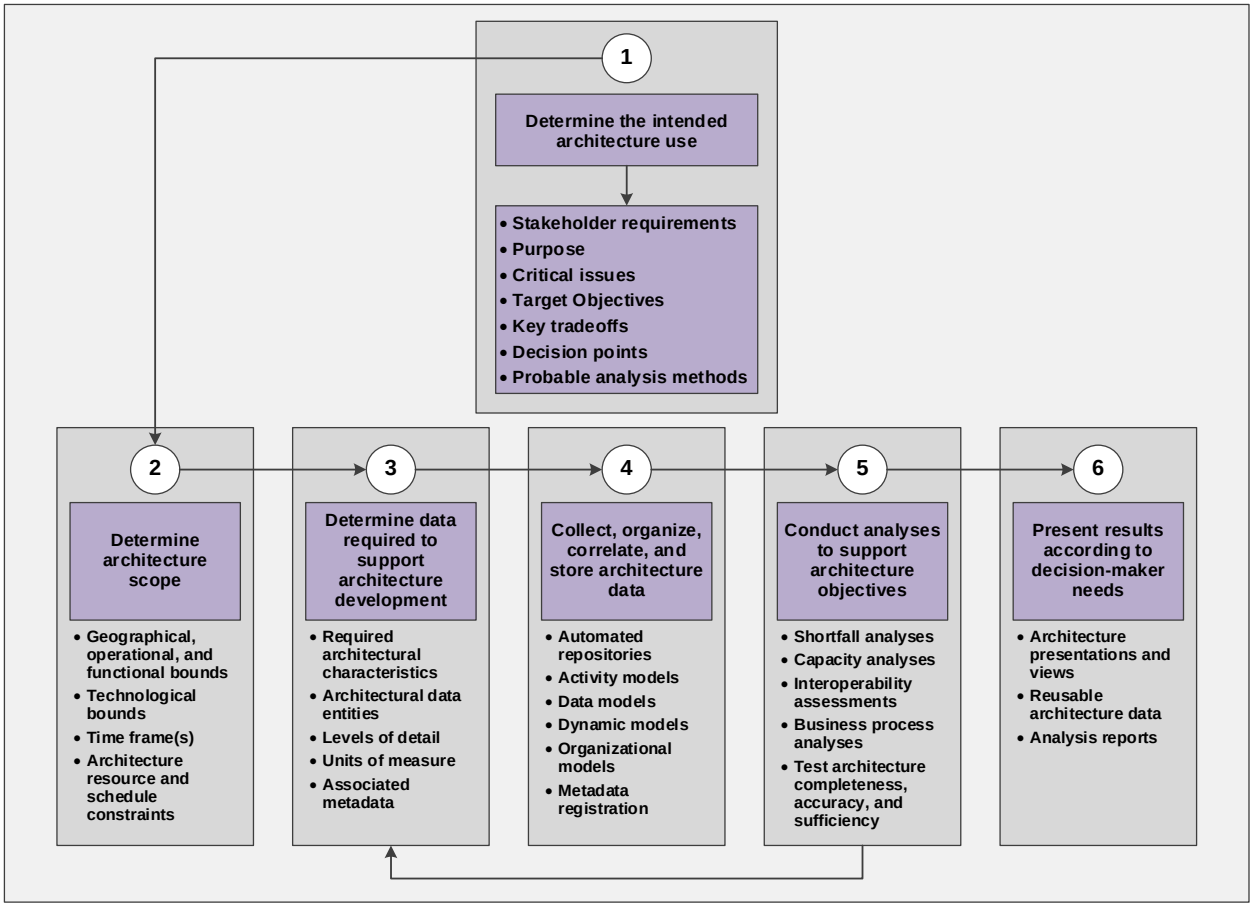

Figure B- 18: DoD Six-Step Architecture Development Process

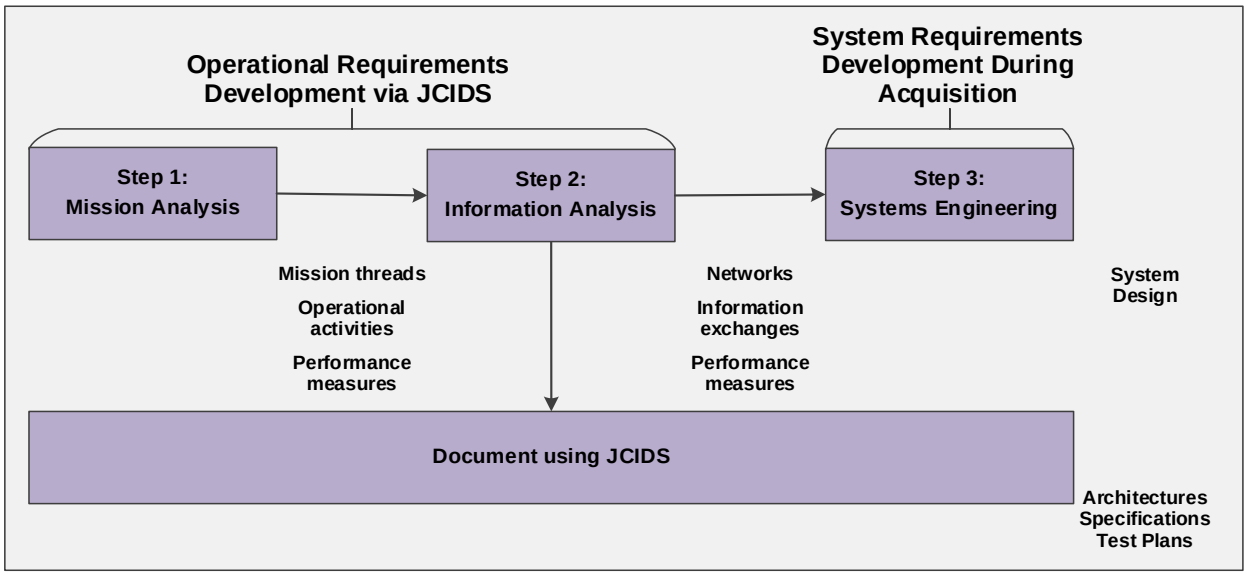

Figure B- 19: Net-Ready Development Applied to the JCIDS and Acquisition Processes

2.4.1. Background. With the release of DoDAF version 2.0, the architecture focus switched from "products" to "data." Similarly, the net-ready certification process changes net-ready architecture development from an architecture product process to a data focus to enable analysis among programs, systems, and services. Architectures for net-ready certification will be developed using the most current DoDAF version or the optional Net-Ready Architecture Data Assessment Template. Sponsors are encouraged to use the WMA Architecture Development Standards IAW Reference [7]). Instructions for the Net-Ready Architecture Data Assessment Template are at the URL in Reference [63].

2.4.1.1. DoDAF Use for Net-Ready Certification. Develop architectures for the net-ready certification using the most current DoDAF version. Existing architectures will be updated to the most current DoDAF version before a successor document is submitted. Data sharing and data interoperability are enabled through architectures. In addition to required architecture data, Reference [7] and associated artifacts/views identified in Figure A-4 for all capability requirements documents, Figure B-20 identifies additional net-ready artifacts/views.

Document[1]	**AV-1**[2]	**DIV-1**	**DIV-2**	**DIV-3**[3]	**SV-1**	**SV-2 or SvcV-2**	**SV-4 or SvcV-4**	**SV-5a**[4] **or SvcV-5**	**SV-6 or SvcV-6**	**SV-7 or SvcV-7**	**StdV-1**[5]	**StdV-2**[5]
CDD	S/P[6]	S[6]	S[6]	P[6]	S/P[6]	P[6]	P[6]	P[6]	S/P[6]	P[6]	P[6]	P[6]
IS-ICD/ IS-CDD[7] **(RDPs/CDs)**	S[6]	N/A[6]	N/A[6]	N/A[6]	S[6]	N/A[6]	N/A[6]	N/A[6]	N/A[6]	P[6]	N/A[6]	N/A[6]

Notes:

[1] The Sponsor provides the OV-2, OV-4, and OV-5a, required by Figure A-4 for all capability requirements documents, together with the SV-1 and SV-2 to determine if the NR certification is applicable. In cases where the Sponsor proposes that the NR certification is not applicable, insert the language "The Sponsor proposes the NR certification is not applicable due to the lack of Joint Interfaces/Information Exchanges. The OV-2, OV-4, OV-5a, and SV-1 or SV-2 are provided for J-6 for review to make the official determination."

[2] Recommend sponsors use AV-1 to describe their architecture IAW Appendix H to Enclosure B.

[3] The DIV-3 must identify system elements that support access to the data source by the DoD enterprise, including Web Service Description Language registration information, service end point, and DoD Meta Data Registry namespace identification.

[4] The SV-5a must align with the OV-5a (or OV-5b). The OV-5a (or OV-5b) must use UJTs (and Service task list extensions, if applicable) for alignment of activities. In cases where the program supports an activity not represented in the UJTL, the shortcomings are to be identified in the activity taxonomy and considered for incorporation upon the next update of the UJTL, in accordance with Reference [8], and using the tools available at the URL in Reference [8]

[5] The technical portion of the StdV-1 and StdV-2 are built using the DoDIN Technical Guidance-DISR standards profiling resources and, within six months of submitting JCIDS documentation, must be current and published for compliance. Use of non-mandated DISR standards in the StdV-1 must be

approved by the PM or other duly designated Component official and documented by a waiver notification provided to the DoD CIO.

[6] S/P: The Sponsor, or operational user/representative, works jointly with the program office (depending upon program stage), to develop the architecture data. DoD Components may have additional architectural/regulatory requirements for CDDs. (e.g., HQDA may require the SV-10c, USMC may require the SV-3, etc.).

S: The Sponsor, or operational user/representative, is responsible for development of the architecture data.

P: The sponsor, or operational user/representative should obtain this architecture data from the program office. DoD Component may have additional architectural/regulatory requirements for CDDs.

N/A: Not Applicable.

[7] IS-ICDs and IS-CDDs are required to provide the DoDAF views associated with the baseline CDDs.

Figure B- 20: Net-Ready Architecture Data and Associated Artifacts/Views

2.4.1.2. Architecture Tools. Produce architectures using a tool that focuses on architectural data rather than only upon individual artifacts/views. Use of COTS architecture tools that can collect, organize, and store the data, and make architecture data and associated artifacts/views available to the federated repository in a non-proprietary manner, is encouraged.

2.4.1.3. Submitting Architectures. Required architecture data and associated artifacts/views are submitted via a URL identified by the Sponsor in the reference section of the document. Architecture data formats and associated artifacts/views support staffing, analysis, distribution, and reuse, and must be submitted in formats that can be viewed without specialized or proprietary tools so they are accessible to and understandable by reviewers. See Reference [7] for guidance on establishing compliant architecture repositories. DoDAF Meta Model (DM2) Physical Exchange Specification (PES) compliant COTS tools are available with architecture data exchange standards, and should be used when possible to develop and submit required architecture data and associated artifacts/views. When using Microsoft products or non-DoDAF PES compliant architecture tools, Sponsors will use architecture data templates provided by appropriate mission area leads for submission of architecture data and traceability to higher-level references and enterprise architectures. Reference [7] is the Architecture Development standard for Warfighting Mission Area. In addition, Reference [7] provides additional Architecture Development granularity standards for the Warfighting Mission Area.

2.4.2. DoD IEA Alignment. The DoD IEA provides a common taxonomy and lexicon to describe required communications capabilities and align solution architecture with the DoDIN as required by Reference [52]. The DoD IEA describes the DoD Information Enterprise as required and defined by Reference [52].] The DoD IEA provides guidance and limitations for solution architectures.

2.4.2.1. Architecture Alignment. Align solution architectures to the laws, regulations, and policies identified in Reference [64] and according to the compliance criteria in the DoD IEA. Show linkage to parent EAs, and fit within

Component and DoD architecture descriptions, using appropriate Reference model and reference architectures (DoD IEA). The URL provided should be complete enough to point to specific architecture artifacts to preclude ambiguity when several versions exist or a large repository is the target of the URL.

2.4.2.2. IEA Architecture Data. For aligning with DoD IEA, architecture data that is within scope of the IEA should be either, 1) the same, 2) extended, 3) traceable, or 4) tailored. System unique architecture data requires a cross-walk table to the DoD IEA data where a relationship exists and is included in the ISP.

2.4.3. Net-Ready Information and Architecture Views. The net-ready architectural developmental process and template is located at the URL in Reference [42].

3. Net-Ready Certification Guide.

3.1. Overview.

3.1.1. This enclosure provides a net-ready certification process overview within the DoD IT lifecycle. Net-Ready assessments are conducted throughout the IT lifecycle to identify and resolve potential interoperability and/or emerging communications and computers challenges and mitigate the risk of delivering non-interoperable capabilities to the Warfighter.

3.1.2. When responsibility to review and certify the net-ready performance attribute is assigned to the Sponsor IAW Enclosure A of this manual, the Sponsor may deviate from this certification guide.

3.1.3. Any substantive changes to this guide will be coordinated with and approved by the DJ-6 or designee.

3.2. Review Process.

3.2.1. The J-6 receives all CDDs and IS-CDDs during initial staffing from the Joint Staff Gatekeeper or via the document's assigned Lead FCB and reviews the NR content.

3.2.1.1. The J-6 recommends to the Joint Staff Gatekeeper whether the net-ready performance attribute (KPP, KSA, or APA) should be designated a JPR. If designated a JPR then the net-ready performance attribute is elevated to a KPP.

3.2.1.2. If designated a JPR by the Joint Staff Gatekeeper, then the J-6 will assess and certify that the system meets net-ready and spectrum requirements compliance.

3.3. Review Criteria.

3.3.1. The J-6 certifies net-ready and spectrum requirements compliance. The J-6 reviews and comments on the ISP, including content of the net-ready summary table, DoDAF architecture data, associated artifacts/views, and

spectrum requirements compliance. DBS documents must comply with the Business Enterprise Architecture (BEA).

3.3.1.1. Pre-Milestone A Documents. Prior to Milestone A, ICDs, IS-ICDs, DCRs, and CONOPS are reviewed by J-6 for several reasons including:

3.3.1.1.1. Identifying JCA, JMT, associated mission areas, and UJTs.

3.3.1.1.2. Determining any interoperability considerations with other developing capabilities.

3.3.1.1.3. Determining if DoDIN goals and characteristics and NETOPS for the DoDIN direction in Reference [54] are addressed.

3.3.1.1.4. Ensuring spectrum requirements are identified IAW References [5] and [42].

3.3.1.1.5. EMSO Requirements are met IAW with References [43] and [65].

3.3.1.2. Post-Milestone A Documents.

3.3.1.2.1. The net-ready performance attribute is certified via KM/DS, using DoDAF architecture data (Reference [7] for architecture development standards), associated artifacts/views, and spectrum requirement compliance. The post Milestone A document certification evaluates compliance with net-ready performance attributes, DoDIN goals and characteristics, capability requirements portfolio management recommendations, and alignment to the current DoDAF. Certification occurs prior to Milestone B and when capability changes result in updates to the net-ready certification. Architecture data and associated artifacts/views are provided via a URL where the architecture is registered for repository access versus incorporating the architecture products in the document. The architecture must be discoverable and accessible per Appendix H of this enclosure.

3.3.1.2.2. Net-Ready Certification also applies to IS-CDD variants outlined in this manual. Initial net-ready certification will occur during the IS-CDD review process. Final net-ready certification must be completed prior to Milestone C.

3.3.1.2.3. The net-ready contained in the ISP is reviewed for recommendation to DoD CIO, including current DoDAF architecture, associated artifacts/views, and spectrum requirements compliance. Sponsors may use the WMA Architecture Development Standards, Reference [7] as a reference for architecture data requirements.

3.3.1.2.4. DBS Document Reviews and Net-Ready Certification. DBS documents are reviewed to determine if JROC interest exists IAW this manual and Reference [36], and to provide comments.

3.4. Process Relationships. Figure B-21 depicts the DoD acquisition, JCIDS, net-ready certification, and spectrum requirement compliance process relationships. The system must have a Joint Interoperability Test Command (JITC) interoperability test certification and/or Component-specific Joint

Interoperability Certification prior to the full rate production decisions IAW Reference [5].

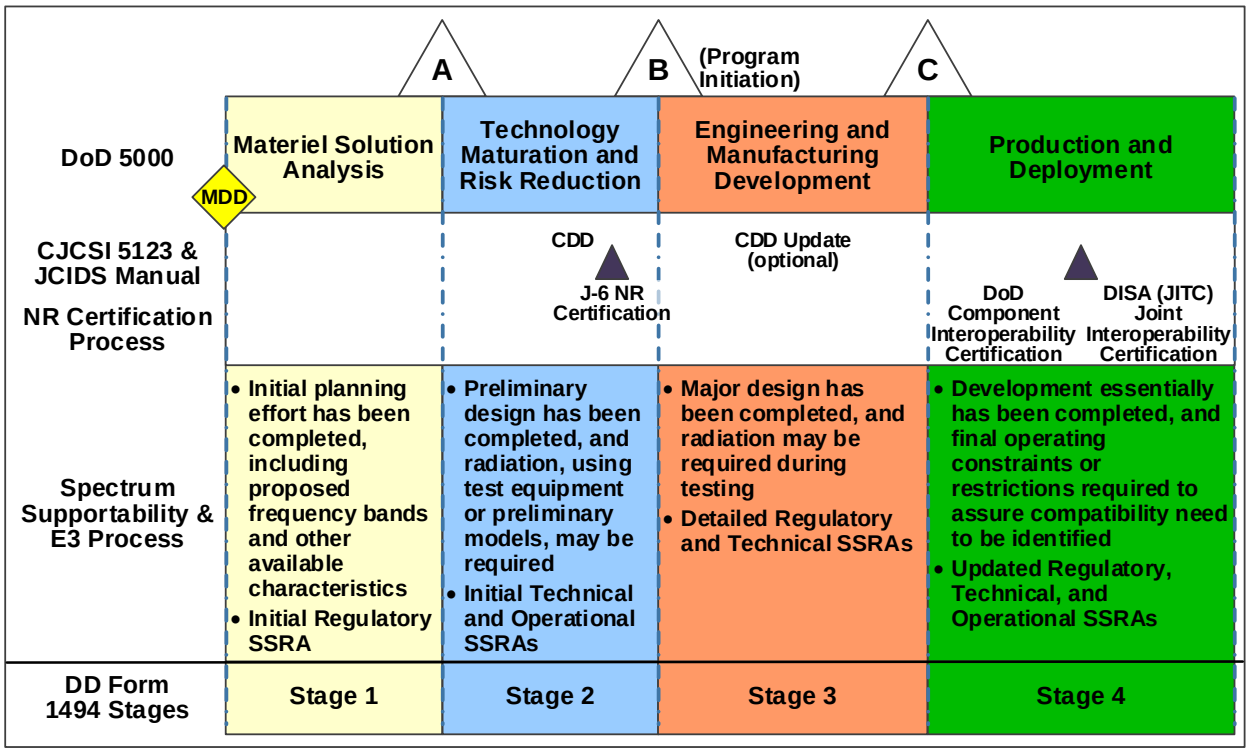

Figure B- 21: DAS, JCIDS, and NR Certification Relationship Overview

3.5. Net-Ready Staffing.

3.5.1. JCIDS Document Review and Certification. Pre-Milestone A JCIDS document reviews, CDD and IS-CDD certification of the net-ready performance attributes, using the DoDAF architecture data, associated artifacts/views, and spectrum compliance is accomplished in concert with JCIDS document staffing. Interoperability issues may be identified by DoD Component via KM/DS.

3.5.2. C4/Cyber FCB Adjudication. Unresolved net-ready certification, DoDAF architecture data per Reference [112], associated artifacts/views, and spectrum compliance issues are forwarded to the C4/Cyber FCB or Military Intelligence Board (MIB) for resolution and their decisions provided to the lead DoD Component to complete the JROC approval process. The C4/Cyber FCB and MIB ensure unresolved issues are presented to the JROC for resolution via the appropriate FCB. Unresolved issues will prevent JCIDS document net-ready certification.

3.6. Types of Net-Ready Certifications. Net-Ready Certification is provided via a J-6 signed memorandum. The three categories are:

3.6.1. Certified. The IT has completed all net-ready requirements and/or stages and all comments were successfully adjudicated. [Note: The J-6 memorandum will specify when the NR performance attribute is sufficient (i.e.,

correct and complete) to support a joint interoperability certification decision (as coordinated with JITC].

3.6.2. Not Certified. The IT has completed all net-ready requirements and/or the stages but has unresolved critical comments that deny certification.

3.6.3. Not Applicable. Consistent with Joint Staff Gatekeeper assigned JSD and guidance in Enclosure A of this manual, the net-ready certification does not require joint certification because it lacks joint interface or does not exchange joint information. The DoD Component will provide Component net-ready certification as required.

3.6.3.1. To facilitate this determination, the Sponsor/program will provide J-6 with the DoDAF SV-2 view to complement the OV-2, OV-4, and OV-5a views provided with the baseline document IAW Figure D-1.

3.6.3.2. The Component will then certify that the IT has met all of the net-ready criteria and integration requirements specified by the Component.

3.6.4. Not Required. The net-ready certification is not required for this stage or type of document IAW this manual.

3.7. Failure to meet net-ready certification requirements. Failure to meet or maintain net-ready certification may result in:

3.7.1. No JROC validation of the program CDD or DoD CIO approval of the ISP.

3.7.2. Recommendation that the IT not proceed to the next acquisition Milestone.

3.7.3. Recommendation that funding be withheld until compliance is achieved and the program and/or system is validated.

3.7.4. Withholding of net-ready certification and recommend revoking any existing Interim Certificate to Operate (ICTO) until the issue is corrected.

3.8. Recommendations. Failed net-ready certification recommendations are provided to USD(R&E); USD(A&S); USD(P); USD(C); the Under Secretary of Defense for Intelligence (USD(I)); Director, CAPE; DoD CIO; DoD EA for Space; and the JROC. Recommendations are also posted to the KM/DS system for visibility and access to other stakeholders.

3.9. Resources. Net-Ready internet resources are located at the URL in Reference [42]. This page will be kept up-to-date as web sites change. Contact the Joint Staff lead if unable to access the resource page.

3.10. Spectrum and E3 Control Requirements Compliance. To obtain a net-ready certification all spectrum dependent devices must comply and be developed with the spectrum management and E3 direction in References [5], [10], [43], [44], [66], and [67]. The assessment of equipment or systems needing spectrum is the receipt of equipment spectrum certification, availability of frequencies for operation, and consideration of EMC. For all

spectrum dependent systems, a SSRA is conducted by the DoD Component to identify spectrum and E3 control risks, review these risks at acquisition milestones, and manage these risks throughout the lifecycle of the system. The spectrum process includes joint, DoD, national, and international policies and procedures for the management and use of the EM spectrum. The spectrum process is at the URL in Reference [42].

3.11. EMSO Requirements. The DoD Spectrum Data Administrator will certify compliance with EMS data sharing requirements as outlined in References [44], [68], and [69]. The AOCO Governance Board shall account for requirements, programming, oversight and guidance as approved by the JROC through the Battlespace Awareness and Force Application Functional Capabilities Board (BA/FA FCB).

ANNEX B TO APPENDIX G TO ENCLOSURE B
FORCE PROTECTION KPP GUIDE

1. Overview. The Force Protection (FP) KPP (one of the four mandatory KPPs) is intended to ensure protection of occupants, users, or other personnel who may be adversely affected by the system or threats to the system. Although the FP KPP may include many of the same attributes as those that contribute to System Survivability, the intent of the FP KPP is to address protection of the system operator or other personnel against kinetic and non-kinetic fires, CBRN, and environmental effects, rather than protection of the system itself and its capabilities.

1.1. Purpose. The purpose of this annex is to provide users with an overview of the required content for the FP KPP and outline the certification process for the FP KPP.

1.2. Applicability. The FP KPP is applicable to CDDs addressing manned systems or systems designed to enhance personnel survivability.

1.3. Proponent. The FP proponent is the Protection FCB, with advisory support from the Office of the Under Secretary of Defense for Personnel and Readiness (USD(P&R)). For questions, please contact the Protection FCB at (703) 693-7116.

2. Force Protection KPP Content Guide. Force protection attributes are those intended to protect the human occupants of manned systems, humans that interface with unoccupied systems, and non-adversary personnel subjected to hostile actions. Use of the FP KPP in a CDD is expected for all manned systems, unmanned systems which interface with or operate in the proximity of personnel and for systems designed to enhance personnel survivability.

2.1. Synergy/Overlap with SS. The FP KPP may include some of the same attributes as those in SS, but the emphasis is on protecting system occupants or other personnel rather than protecting the system itself. As such, the levels of performance attributes in FP are generally higher than those in SS. (i.e., inability to continue the mission where the occupants or other non-adversary personnel are protected from becoming casualties is generally preferable to cases where the system remains mission capable, but the occupants or other non-adversary personnel in the vicinity become casualties.)

2.2. Exclusion of Offensive Capabilities. Offensive capabilities that are primarily intended to defeat adversary forces before they can engage non-adversary forces are not included as a FP attribute.

2.3. Tailoring of Standards. For attributes listed below which have an associated protection standard identified, compliance with the standard is expected unless the operational context for the capability solution indicates

that a higher or lower standard of force protection is more appropriate. In cases where a deviation from the standard is appropriate, the

FP KPP will identify the tailored levels of required force protection, along with rationale as to why the operational context makes a different level of protection appropriate.

2.4. Force Protection Attributes. Attributes for FP fall into five general categories that must be addressed when applicable to the system under consideration – either as a feature designed into the system or mandated as protective equipment used by personnel exposed to the applicable threats.

2.4.1. Protection from kinetic fires. Attributes include: Level of armor protection; Munitions (sizes) which are ineffective; Level of shock/blast that is survivable; and Level of fire/flame resistance.

2.4.2. Protection from non-kinetic fires (other than CBRN). Attributes include: Standards for protection from lasers/dazzlers/eye-safety (with or without PPE) are outlined in Reference [70];

2.4.3. Protection from CBRN effects. Applicable to required systems to operate through CBRN environments IAW Reference [71]. Attributes include: Detection and identification; Air filtration and/or pressurization; Medical prophylaxes and/or countermeasures; Decontamination/recovery capabilities; and Nuclear survivability for systems covered under Reference [72]; and Protection from EM attack physiological effect, including ability to maintain functionality during high level EM exposure or EMP conditions.

2.4.4. Protection from environmental effects. General standards are outlined in References [73] and [74]. Attributes include: Standards for acceptable pressure/oxygen levels for personnel, including pressurization and/or supplemental oxygen are outlined in Reference [75]; Acceptable temperature limits for personnel (with or without PPE); Standards for acceptable vibration/acoustic limits for personnel (with or without PPE) are outlined in Reference [76]; and Acceptable G-force loading limits for personnel (with or without PPE) under normal operations.

2.4.5. Protection from crash events. Attributes include: Standards for crash survivable G-force loading limits for personnel (with or without PPE) are outlined in Reference [77]; Protection from impact trauma, including seats and retaining systems; Preservation of occupied space; and Protection from post-crash fuel spills and fires.

3. Force Protection KPP Endorsement Guide. This guide provides procedures for the Chair of the Protection FCB to review the FP KPP during the staffing of capability requirements documents. When responsibility to review and endorse the FP KPP is assigned to the Sponsor IAW Enclosure A of this manual, the Sponsor may deviate from this endorsement guide. Any substantive changes to this guide will be coordinated with and approved by the DJ-8 or designee.

3.1. Review Process.

3.1.1. The Protection FCB receives, via the KM/DS system, all JROC Interest or JCB Interest documents.

3.1.2. The Protection FCB reviews the FP KPP and recommends to the Joint Staff Gatekeeper whether or not the FP KPP should be designated a JPR.

3.1.2.1. If designated a JPR then the Protection FCB assesses the FP KPP, with advisory support from the Office of USD(P&R), and determines if requirements for protecting system operator and other personnel under applicable threat environments are adequately described.

3.1.3. The Protection FCB reaches out to the Sponsor for further clarification, if needed.

3.1.4. The Protection FCB provides a FP KPP Endorsement, documents rejection of the FP KPP Endorsement, or provides a waiver.

3.2. Review Criteria.

3.2.1. Is there evidence of a comprehensive analysis of the system and its planned use, including the planned operating environment, operating tempo, threat, vulnerability assessment, and solutions leading to the determination of the value? Are the analyses of these assumptions supporting the FP KPP documented?

3.2.2. Are the FP attributes and associated values consistent with the intended operational use of the system (i.e., the CONOPS)? Relative to the FP categories identified in this annex:

3.2.2.1. Are the occupants adequately protected from kinetic fires, and are the identified attributes and associated values appropriate given the operational context?

3.2.2.2. Are the occupants adequately protected from non-kinetic fires (other than CBRN), given the operational context? Are the attributes and associated values in compliance with the standards identified in this annex or are deviations justified in light of the operational context?

3.2.2.3. Are the occupants adequately protected from CBRN effects, given the operational context? Are the attributes and associated values in compliance with the standards identified in this annex or are deviations justified in light of the operational context?

3.2.2.4. Are the occupants adequately protected from environmental effects, given the operational context? Are the attributes and associated values in compliance with the standards identified in this annex or are deviations justified in light of the operational context?

3.2.2.5. Are the occupants adequately protected from crash events, given the operational context? Are the attributes and associated values in compliance with the standards identified in this annex or are deviations justified in light of the operational context?

3.3. Endorsement Documentation. Upon successfully FP KPP Endorsement, the Protection FCB Chair will provide the Sponsor with an endorsement memorandum that will be included with the JCIDS document and maintained within the KM/DS system.

ANNEX C TO APPENDIX G TO ENCLOSURE B
SYSTEM SURVIVABILITY KPP GUIDE

1. Overview. The SS KPP (one of the four mandatory KPPs) is intended to promote the development of critical warfighter capability that can survive kinetic (i.e., traditional, non-traditional, and CBRN) and non-kinetic (cyber and electromagnetic spectrum (EMS)) threats across domains and applicable environment including space. The SS KPP supports three system oriented objectives: prevention, mitigation in tactically relevant time, and recovery from threats and fires. Simultaneously, the SS KPP maintains survivability from diverse environmental factors (i.e., heat, dust, moisture, EMS-congested areas, etc.). The SS KPP promotes the analysis of probable threats and advances a SoS approach that leverages in-depth, overlapped, or redundant defensive capabilities through networked, autonomous, or semi-autonomous systems to ensure mission completion, despite the loss or degradation of individual components.

1.1. Purpose. The purpose of this annex is to provide users with an overview of the required content and compliance steps for the SS KPP endorsement.

1.2. Applicability. The SS KPP is applicable to all CDDs, including IS-CDDs. Certain precursor steps and requirement development activities are appropriate for inclusion in ICDs. In the event of a CIP breach, the SS KPP will be reviewed and reassessed for survivability based on updated threat information.

1.3. Proponent. The SS proponent is the Protection FCB. For questions, please contact the Protection FCB at (703) 693-7116.

2. System Survivability KPP Content Guide.

2.1. The SS KPP ensures that systems are designed to enable critical warfighter capabilities that can prevent, mitigate, and recover from adversarial threats or from detrimental environmental conditions. The primary objective is to protect warfighter systems and promote system survivability within the full spectrum of operating environments:

2.1.1. The warfighter system survivability requirements seek to:

2.1.1.1. Prevent or thwart attacks; Defined as the ability to neutralize imminent or actual attacks and their effects. This can include broad methods that prevent attack or their effects through stealth (camouflage, concealment, and deception); warning and situational awareness; maneuver and operational agility; improved security; and hardening against nuclear weapons effects.

2.1.1.2. Mitigate or reduce vulnerabilities in tactical relevant time from threats and fires. Mitigate the negative effect of attacks in tactically relevant timeframes. Defined as the ability to minimize the effects, and manage the consequence of attacks in timeframes that are necessary for mission completion and success. Additional mitigation methods might include

countermeasures, graceful degradation, redundancy, resiliency, hardening, strengthening, and preserving system capability.

2.1.1.3. Recover to a known good condition between mission cycles to fight another day. Recovery is the ability to restore to a known good condition between mission cycles and incorporate any updated changes to counter newly identified risks to mission completion. Methods that enable recovery include system restoration, repair, replacement, update and reconstitution.

2.1.2. System survivability within the operating environment encompasses:

2.1.2.1. Development of capabilities that can survive kinetic, non-kinetic attacks and environmental variables (heat, dust, moisture, EMS, congestion, corrupted power, corrupted data, etc.) in all domains including space.

2.1.2.2. The ability of a system to avoid, withstand, and/or operate during and after exposure to chemical, biological, radiological, and nuclear (CBRN) environments, including EMP.

2.1.2.3. Exposure to cyber- or EMS-attacks or exposure to fires that prevent or retard the completion of critical operational missions by destruction, corruption, denial, or exposure of transmitted, processed, or stored information.

2.2. Scope. To adequately address the various forms of threats the SS KPP is divided into three focus elements: Kinetic Survivability, Cyber Survivability, and EMS Survivability. Each of these focus areas include various attributes and elements to help define and address the prevailing threats in their unique battlespace. *It is also important to match the level of survivability with the system's unmitigated vulnerabilities and forecasted threats in the most stressful and demanding operational environments*.

2.3. Synergy and overlap with the FP KPP and Sustainment KPP. The SS KPP may include some of the same attributes as those in FP KPP, however, the emphasis of the SS KPP is on maintaining the mission capabilities of the system as defined in the CONOPS through the applicable threat environment rather than protecting system occupants or other personnel. The SS KPP also complements the Reliability performance attribute defined in the Sustainment Guide under Annex D to Appendix G of this enclosure. Depending upon their scope and purpose, requirements and performance attributes designed to meet one may also meet the other.

2.4. SS KPP Compliance Steps. Every system under consideration will have some aspect to which the SS KPP applies. However, not all systems will need to comply with the requirements of all three-focus areas. There are five basic steps needed to comply that are common to all three focus areas. See the individual focus area guidebooks for additional guidance. The five basic steps are:

2.4.1. Determine Applicability. Sponsors must determine which components of system survivability are applicable to their proposed system. The

operational environment in which that system will operate and the mission type and criticality should be considered. Typically, this can be obtained from the system CONOPS.

2.4.2. Assess the Threats. All likely threats (both kinetic and non-kinetic) that a system may face should be explored and documented in a system threat assessment. Kinetic threats can span land, sea, air, and space as well as CBRN, while non-kinetic include Cyber and EMS. Threat assessments shall be used to inform system requirements, risk mitigations, and trade-offs. Assessments should be documented by the VOLT report through an Online Threat Assessment Tool or equivalent report.

2.4.3. Determine the level of risk. Determined by evaluating multiple contributing factors and then deriving an overall risk category. This process identifies appropriate strength of implementation levels for survivability. A higher risk assessment will increase the expectation for more extensive and detailed requirements and more robust protection, mitigation, and recovery efforts.

2.4.4. Develop Requirements. Specify system requirements for each applicable SS attribute. Develop clear, specific and achievable requirements for system components, features and technologies that will contribute to mission success against identified threats. If performance criteria are specified, ensure that they include threshold and objective measures that are realistic, testable, and measurable.

2.4.5. Apply Risk Management. Use the data gathered in steps (1) through (4) to inform a holistic strategy for ensuring the survivability of the system. Then assess this strategy against the limitations of cost, schedule, and performance in order to make informed decisions about what level of survivability is realistically achievable and which requirements should be included.

2.5. Elements of the SS KPP endorsement. The key elements of system survivability are the attributes associated with Kinetic, Cyber, and EMS survivability and their associated attributes.

2.5.1. Kinetic Survivability. Applies to all land, sea, air, and space systems that are vulnerable to kinetic adversary threats from the smallest caliber bullet to the most sophisticated ballistic missile. Kinetic Survivability includes CBRN, Space, and environmental considerations that depend on Kinetic Survivability Attributes that all contribute to producing a highly survivable design:

2.5.1.1. CBRN Considerations. The sponsor will state whether the system has been designated mission critical. If the system is mission critical and must survive and/or operate in CBRN environments, the sponsor will designate the system as “CBRN Mission Critical” per Reference [71]. The sponsor must include a brief rationale justifying this designation or its absence for all systems. If designated CBRN Mission Critical, the system must consider all relevant CBRN environments, as well as operational and maintenance

requirements relating to ensuring hardness against those CBRN environments. For CBRN Mission Critical systems, CBRN survivability attributes should not be addressed as Other System Attributes, but included within the System Survivability KPP, as a KSA, or as an APA.

2.5.1.2. Space Considerations. Space mission assurance is intended to deter aggression, promote stability and responsible use of space. The required level of space mission assurance will be based on type of operation supported and the Assured Space Framework. This includes the three-tier approach to determine level of importance of survivability while making tradeoffs among cost, schedule, and performance. Per Reference [78] these tiers must be used within the JCIDS process to attribute space mission assurance level to space mission capabilities. Following these three tiers, the system must be:

2.5.1.2.1. Endurable, survivable, and continuously available through all phases of conflict and levels of hostility (Tier 1).

2.5.1.2.2. Present through all phases and levels of conflict and able to mitigate attack effects during the mission, with possible quality and quantity limitations and transient or localized outages; capable of recovery on tactical timelines (Tier 2).

2.5.1.2.3. Restorable based on rear echelon and support homeland security needs but could be lost during highest levels of conflict (Tier 3).

2.5.1.3. Environmental Considerations: Sufficient requirements shall be specified to ensure that environmental factors will not easily or unnecessarily damage a system to degrade its ability to perform its intended mission.

For More Information pertaining to kinetic survivability, see the Kinetic Survivability Guidebook via KM/DS, Reference [4].

2.5.2. Cyber Survivability. Ensures warfighter systems are designed to prevent, mitigate, and recover from cyber-attacks by applying a risk managed approach to building and maintaining systems.

2.5.2.1. The threat methodology employed by a cyber-review broadly accounts for mission type, cyber dependency level of the system, adversary threat tier, and impact level of system compromise in determining a Cyber Survivability Risk Category (CSRC) that identifies appropriate strength of implementation levels.

2.5.2.2. Accomplished through the following Cyber Survivability Attributes (CSAs), as appropriate, to support the SS pillars of prevent, mitigate, and recover:

2.5.2.2.1. Prevent – CSA-01: Control Access; CSA-02: Reduce System's Cyber Detectability; CA-03: Secure Transmissions and Communications; CSA-04: Protect System's Information from Exploitation, CSA-05: Partition and Ensure Critical Functions at Mission Completion Performance Levels; CSA-06: Minimize and Harden Attack Surfaces.

2.5.2.2.2. Mitigate – CSA-07: Baseline and Monitor Systems and Detect Anomalies; CSA-08: Manage System Performance if Degraded by Cyber Events.

2.5.2.2.3. Recover – CSA-09: System Capabilities; CSA-10: Actively Manage System's Configuration to Counter Vulnerabilities at Tactically Relevant Speeds.

For more information pertaining to cyber survivability, threat methodology, Cyber Survivability Risk Category, Example language and applicable CSAs, see the CSE Implementation Guide, via KM/DS, Reference [4].

2.5.3. EMS Survivability. Applies to all systems that incorporate electrical or electronic components that might be susceptible to electromagnetic effects. However, not all of the EMS survivability attributes will apply to all systems.

2.5.3.1. There are five EMS survivability attributes: Spectrum Protection System Adaptability, Spectrum Access Flexibility, Spectrum Efficiency, and Multi-Functionality. All systems that are vulnerable to adversarial employment of the EMS must comply with the Spectrum Protection attribute requirements, while only Spectrum Dependent Systems (SDS) (defined for this purpose as those that operate in the radio frequency (RF) portion of the spectrum) must comply with all five of these attributes.

2.5.3.2. The EMS Survivability Guidebook provides extensive examples of technologies, components and features that help make a system more survivable against EMS threats. It also provides a methodology to assess risk, sample requirements statements, sample performance criteria and compliance tips.

For more information pertaining to EMS Survivability, threat methodology, EMS Survivability Risk Category, Example language, and applicable SSAs, see the EMS Survivability Guidebook, via KM/DS, Reference [4].

3. System Survivability KPP Endorsement Guide. This guide provides procedures for the Joint Staff J-8 Deputy Director for Force Protection (J-8/DDFP) to review the SS KPP during the staffing of JCIDS documents. When responsibility to review and endorse the SS KPP is assigned to the Sponsor IAW Enclosure A of this manual, the Sponsor may deviate from this endorsement guide. Any substantive changes to this guide will be coordinated with and approved by the DJ-8 or designee.

3.1. Review Process.

3.1.1. The Protection FCB receives, via the KM/DS systems, all JROC Interest or JCB Interest documents.

3.1.2. The Protection FCB reviews and assesses the SS KPP and recommends to the Joint Staff Gatekeeper whether the SS KPP should be designated a JPR.

3.1.3. If designated a JPR then the Protection FCB reviews and assesses the SS KPP for compliance with the SS Content Guide and associated Kinetic Survivability, Cyber Survivability, and Spectrum Survivability Guidebooks.

3.1.4. The Protection FCB may also:

3.1.4.1. Determine if requirements adequately describe system survivability attributes needed to be maintained under applicable threat environments.

3.1.4.2. Seek technical guidance and opinion from appropriate subject matter experts and/or communities of interest.

3.1.4.3. Reach out to the Sponsor for further clarification and coordination.

3.1.4.4. Endorse, reject, or provide a waiver for the application.

3.2. Review Criteria.

3.2.1. Is there evidence of a comprehensive analysis of the system and its intended use, including the planned operating environment, operating tempo, threat, vulnerability assessment, and solutions leading to the consideration towards System Survivability? Is the analysis of these factors and conclusions documented?

3.2.2. Are the required items for the SS KPP included in the appropriate sections of the capability requirements document? Are all of the applicable survivability attributes addressed?

3.2.3. Are the SS performance attributes consistent with the intended operational use of the system (i.e., the CONOPS)? Are their criteria realistic, measurable and testable?

3.2.4. Are sufficient requirements specified to mitigate the identified risks?

ANNEX D TO APPENDIX G TO ENCLOSURE B
SUSTAINMENT KPP GUIDE

1. Overview.

1.1. Purpose. This guide provides requirements managers a guide to assist them in ensuring that effective sustainment is addressed and achieved. This is accomplished through compliance with the sustainment metrics as identified in the capability requirements documents. This guide does not prescribe what will be provided to satisfy sustainment requirements but provides factors to be considered when determining if the rationale being provided meets the rigor needed for programs requiring a sustainment metric. The methodology used to establish the Sustainment KPP will be reviewed and shall include sufficient supporting documentation. Reference [51] will assist Sponsors and PMs in developing the Sustainment KPP.

1.2. Applicability. The Sustainment KPP is applicable to all CDDs.

1.3. Proponent. The proponent for the Sustainment KPP is the Joint Staff J-4/Maintenance, Materiel, and Services Division (J-4/MMSD), with analytical support from the Office of the Assistant Secretary of Defense for Logistics and Materiel Readiness (OASD(L&MR)). For questions regarding the Sustainment KPP, contact the J-4/MMSD at (703) 614-0161.

2. Sustainment KPP Content Guide. Sustainment is a key component of performance. Including sustainment planning early during design and procurement enables the requirements and acquisition communities to provide a system with optimal availability and reliability to the warfighter at an affordable lifecycle cost. The value of the Sustainment KPP is derived from the capability requirements of the system, assumptions for its operational context and intended use, and the planned logistical support. Fully developed sustainment objectives allow the PM to develop a solution to satisfy the warfighter requirements and system performance to be measured against standardized metrics.

2.1. Background. The tenets of lifecycle management emphasize sustainment planning early in the capability solution's lifecycle, including requirement generation activities. Lifecycle management is the implementation, management, and oversight by the PM of all activities associated with the acquisition, development, production, fielding, sustaining, and disposal of a DoD system. This guide emphasizes those sustainment analyses, activities, and documents necessary to ensure the design, development, testing, production, and fielding of reliable, affordable, and maintainable systems. The criteria, information, and activities listed are not inclusive – that is, they cannot necessarily be applied to all systems. The Sponsor, together with the PM, must determine whether and how each item is applicable to its concept,

technology, and/or system, although sufficient sustainment metrics to ensure a viable, cost-effective, and supportable system must be incorporated.

2.2. Development of the Sustainment KPP.

2.2.1. The Sustainment KPP is derived from system availability requirements to support the required capability, assumptions for its design and operational use as specified in the CONOPS and/or OMS/MP tradeoffs between reliability, maintenance concepts, lifecycle cost, and the planned sustainment strategy. In order for the PM to develop a complete system to provide warfighting capability, sustainment attributes must be established and performance of the entire system measured against those metrics. The Sustainment KPP is comprised of several mandatory components: Materiel Availability and Operational Availability, and three mandatory attributes (either KSAs or APAs): Reliability, Maintainability, and the O&S cost. Respectively, they provide fleet level wide availability and operational availability. The operational framework for the expected Materiel and Operational Availability must be clearly articulated during the AoA or similar studies and based on the operational context in the validated ICD and/or OMS/MP. For example, if a CCMD has capability requirements which lead to the development of a new medium lift transport vehicle, knowledge of the range of missions and required duration; limitations on loading and capacities; knowledge of operating environments and other related mission criteria are essential to ensure developers consider the variables that affect the Sustainment KPP.

2.2.2. Operational Framework. During the AoA or similar study, the operational framework guides the development of alternative materiel and non-materiel solutions (including hardware/software systems) and alternative sustainment approaches. Assessment of capability requirements and performance metrics must consider both the system and its sustaining support at the same time. Additionally, the AoA or similar study must consider the sustainment requirements of the system, including factors such as availability, reliability, maintainability, and O&S costs.

2.2.3. Elements of the Sustainment KPP. The Sustainment KPP is supported by several elements that provide an integrated structure that balances sustainment with capability and affordability across a capability solution's lifecycle and informs decision makers in trade-off analysis. These elements are comprised of the following mandatory components: Material Availability and Operational Availability, and mandatory attributes (KSAs or APAs): Reliability, Maintainability, and O&S cost. See Reference [51] for additional guidance on the following elements:

2.2.3.1. Materiel Availability. Materiel Availability is the measure of the percentage of the total inventory of a system operationally capable, based on materiel condition, of performing an assigned mission. This can be expressed mathematically as the number of operationally available end items/total population. The total system population includes all operational systems

necessary to support the Operational Context of the CDD including operational systems for training (vice mock-ups, partial systems, and simulators), systems for attrition reserve and prepositioning, and systems temporarily in a non-operational materiel condition, such as planned depot maintenance. Materiel Availability requirement links directly with investment decisions, as the total quantity purchased is informed by the sustainment strategy and how many systems will be in available status to support CONOPS and OPLANS. Materiel Availability also covers the timeframe from placement into operational service through the planned end of service life. Materiel Availability takes into account all calendar time that a system is in the inventory, including "out-of-reporting" status. For single or small-quantity systems, Materiel Availability can represent available time (i.e., up time, when the system is in operational status) as a percentage of total calendar time.

2.2.3.1.1. Materiel Availability is typically not applicable to AIS systems. See Figure B-23 for additional guidance on AIS IS-CDD Sustainment definitions.

2.2.3.1.2. Figure B-22 provides an example of a single location to display total system inventory requirements and may be modified to reflect each system's inventory requirements.

	CONOPS	Training	Attrition	Prepositioned	Average Annual Down[1]	Total
CONUS						
OCONUS						
Total						

Note:
[1] The average number of unavailable assigned assets based on assumed planned depot/ shipyard cycles.

Figure B- 22: Total System Inventory

2.2.3.2. Operational Availability. Operational Availability is the measure of the percentage of time that a system or group of systems within a unit are operationally capable of performing an assigned mission and can be expressed as (uptime/ (uptime + downtime)). Operational Availability is usually specified for a given scenario or type of unit, e.g., combat group wartime scenario, peacetime training unit, etc. It is normally based on a steady-state situation, usually expressed in terms of annual usage. Determining the optimum value for Operational Availability requires a comprehensive analysis of the system and its planned CONOPS and/or OMS/MP, including the planned operating environment, operating tempo, reliability and maintenance concepts, and supply chain solutions.

2.2.3.3. Reliability Attribute (KSA or APA). Reliability is a measure of the probability that the system will perform without failure over a specific interval, under specified conditions. Reliability shall be sufficient to support the warfighting capability requirements, within expected operating environments. Considerations of reliability must support both availability metrics and be reflected in the O&S Cost attribute.

2.2.3.3.1. More than one reliability metric may be specified, as KSAs and/or APAs, for a system as appropriate. See Figure B-23 for examples of metrics for different types of systems and Reference [51] for further information and instruction. In all cases, the Sponsor shall define criteria that constitute failures.

2.2.3.3.2. For continuous use systems (such as an aircraft), reliability should be measured in terms of its primary usage metric (such as operating hours, miles or flight hours). For discrete systems (such as a single use munition), reliability should be measured as a probability.

2.2.3.3.3. For AIS, a reliability attribute should not use traditional reliability metrics (e.g., MTBF, MTBCF). For appropriate metrics to use for AIS, refer to Figure B-23.

2.2.3.3.4. Mission Reliability. The measure of the ability of an item to perform its required function for the duration of a specified mission profile, defined as the probability that the system will not fail to complete the mission, considering all possible redundant modes of operation.

2.2.3.3.5. Logistics Reliability. Logistics Reliability is the measure of the ability of an item to operate without placing a demand on the logistics support structure for repair or adjustment, including all failures to the system and maintenance demand as a result of system operations. Logistics Reliability is a fundamental component of an O&S cost as well as Materiel Availability.

2.2.3.3.5.1. All indicated and recorded failures, even those that do not affect successful completion of a mission, eventually result in some corrective action. Corrective action often includes some level of repair or inspection to mitigate the failure. Logistics reliability (sometimes called basic reliability) deals with all failures. Repair (called corrective maintenance), in this case can consist of removal and replacement, in-place repair, or some combination thereof for the failed item. The cost of high failure rates can consist of:

2.2.3.3.5.1.1. The need for more spares;

2.2.3.3.5.1.2. The need for additional maintenance personnel;

2.2.3.3.5.1.3. More system downtime;

2.2.3.3.5.1.4. Larger logistics footprint;

2.2.3.3.5.1.5. Decreased readiness to perform missions or increased forces size; and higher lifecycle cost;

2.2.3.3.5.1.6. The need for corrective action on poor reliability or BIT false alarms.

2.2.3.4. Maintainability Attribute (KSA or APA). The measure of the ability of the system to be brought back to a readiness status and state of normal function. Subordinate attributes which may be considered as KSAs or APAs:

2.2.3.4.1. Corrective Maintenance – The ability of the system to be brought back to a state of normal function or utility, at any level of repair, when using prescribed procedures and resources.

2.2.3.4.1.1. All failures – Total elapsed corrective maintenance time (clock hours) for active repair performed as a result of any failure, divided by the total number of failures.

2.2.3.4.1.2. Mission failures – Total elapsed corrective maintenance time (clock hours) for active repair performed as a result of a mission failure, divided by the total number of mission failures.

2.2.3.4.2. Maintenance Burden – a measure of the maintainability parameter related to item demand for maintenance manpower. The sum directed maintenance man hours (corrective and preventive), divided by the total number of operating hours.

2.2.3.4.3. Built in Test (BIT).

2.2.3.4.3.1. Fault Detection (FD) - A measure of recorded BIT indications which lead to confirmed hardware failures. Percent BIT FD is defined as the total number of BIT detected failures divided by the total number of failures then multiplied by 100.

2.2.3.4.3.2. Fault Isolation (FI) – A measure of recorded BIT indications which correctly identifies the faulty replaceable unit. Percent BIT FI is defined as the total number of failures correctly isolated divided by the total number of BIT detected failures then multiplied by 100.

2.2.3.4.3.3. False Alarms (FA) – A measure of recorded BIT indications showing a failure when none has occurred. Can either be expressed as the total number of operating hours divided by the total number of false alarms or total number of FAs divided by total BIT indications then multiplied by 100.

2.2.3.4.3.4. Prognostics – the design ability of the system to proactively predict maintenance issues based on usage, time, actual performance and other factors. This attribute is enabled by data from sensors, health and condition monitoring, communications and human interface capabilities. Prognostics supports Condition Based Maintenance sustainment strategies.

2.2.3.5. O&S Cost Attribute (KSA or APA). Measuring O&S cost provides balance to the sustainment solution by ensuring that the total O&S costs across the projected lifecycle associated with availability and reliability are considered in making decisions.

2.2.3.5.1. The O&S Cost attribute is to be computed using base year dollars. For consistency and to capitalize on other efforts in this area, all CAPE O&S cost elements, outlined in Reference [79], will be used in support of this APA. Energy costs shall be included in O&S cost and will use the base year price throughout the assessment. All O&S costs are to be included regardless of funding source or management control.

2.2.3.5.2. The O&S cost covers the planned O&S timeframe, consistent with the timeframe and system population identified in the Sustainment performance attribute. The O&S Cost APA objective values are to be calculated in base year dollars as 10 percent less than the threshold value. As part of the supporting rationale, provide the annual cost per system (for large systems such as aircraft, vehicles, ships, etc.) or fleet of systems (for networks or smaller systems such as munitions) upon which the O&S Cost APA total is based.

2.2.3.5.3. Submit documentation of sufficient detail to explain all assumptions, data, and methodologies used to develop the threshold estimate values into KM/DS for archival and reference purposes. Programs must plan for maintaining the traceability of costs incurred to estimates and must plan for testing and evaluation. The Sponsor shall plan to monitor, collect, and validate operating and support cost data to support the O&S Cost APA.

2.2.3.6. Logistics Footprint – this optional attribute is a useful metric for measuring the materiel, mobility, and required space to effectively deploy, sustain, or move a weapons system. Incorporating Logistics Footprint in requirements drives design decisions that included actual usage limitations. Measurable elements include inventory/equipment, personnel (government and contractor), facilities, transportation assets, and real estate. Representative elements included in the quantification of logistics footprint include weight (e.g., total weight of deployable consumables, support equipment, energy and spares); personnel (e.g., total number of support personnel in the deployed area); and volume (total volume of deployable consumables, support equipment, energy, and spares).

2.3. Sustainment KPP for complex systems. For complex systems and SoS, the Sustainment KPP and supporting Reliability attribute are to be applied to each major end item or configuration item, and whenever practical, to the system/SoS as a whole. For example, for a highly distributed complex network, the “network availability” (that is, availability of the network function to the user) may be a warfighter requirement but will be difficult to evaluate in test, but a simple linear network to complete a kill chain can be assessed. The Sustainment attribute and Reliability attribute are to be derived and applied to individual nodes of the network. Ship platforms, unmanned aircraft systems, and satellite constellations are other examples. The O&S Cost APA, however, is to be applied to the whole program and not to individual configuration items, unless there are multiple documented subprograms.

2.4. Documentation. A Reliability, Availability, Maintainability, and Cost (RAM-C) report, as defined in Reference [51], will document the quantitative basis for the elements of the Sustainment KPP as well as the technical feasibility tradeoffs and rationale made with respect to system performance, program costs and schedule.

2.5. Development Guide. A guide for developing the appropriate sustainment metrics for different categories of systems is provided in Figure B-23 as an aid for the Sustainment KPP.

3. Sustainment KPP Endorsement Guide. This guide provides procedures for the J-4/MMSD to review the Sustainment KPP during the staffing of a capability requirements document. When responsibility to review and endorse the Sustainment KPP is assigned to the Sponsor IAW Enclosure A of this manual, the Sponsor may deviate from this endorsement guide. Any substantive changes to this guide will be coordinated with and approved by the Director, Joint Staff J-4 Directorate for Logistics (DJ-4) or designee.

3.1. Review Process.

3.1.1. The Logistics FCB gets notification from the Joint Staff Gatekeeper that there is a CDD with a Sustainment KPP that may have joint equity.

3.1.2. The Logistics FCB, in consultation with the Lead FCB, reviews the Sustainment KPP and recommends to the Joint Staff Gatekeeper whether it should be designated a JPR.

3.1.3. J-4/MMSD receives notification of the CDD via the KM/DS system.

3.1.4. J-4/MMSD reviews and coordinates with OASD(L&MR) for Sustainment KPP analysis.

3.1.5. J-4/MMSD consolidates and enters comments into the KM/DS system.

3.1.6. Program Sponsors will contact J-4/MMSD for comment adjudication.

3.1.7. J-4/MMSD and OASD(L&MR) will provide representation to JROC and subordinate boards for unresolved critical comments.

3.2. Review Criteria.

3.2.1. Materiel Availability Attribute.

3.2.1.1. Is there evidence of a comprehensive analysis of the system and its planned use, including the planned operating environment, operating tempo, reliability alternatives, maintenance approaches, and supply chain solutions leading to the determination of the materiel availability value? Are the analysis assumptions documented?

3.2.1.2. Is the total population of systems being acquired for operational use documented, including those in storage or used for training?

3.2.1.3. Are definitions provided for failures, mission-critical systems, and criteria for counting assets as “up” or “down?” Are the failure rate values supported by analysis?

3.2.1.4. Does the metric clearly define and account for the intended service life of the total inventory, from initial placement into service through the planned removal from service? A graphic representation, such as a timeline or sand chart, of the lifecycle profile is an effective way to present the data.

3.2.1.5. What is the overall sustainment CONOPS? Is it consistent with SSA products, including Service and Joint Concepts, CONOPS, and/or OMS/MP, design reference missions, etc. being supported? Is it traceable to the original capability requirements, or agreement with the warfighting community? What alternatives were considered? Have surge/deployment acceleration requirements been identified and are they factors in development of the Materiel Availability metric?

3.2.1.6. Is failure/down-time defined? Is planned downtime (all causes) identified and included? Does analysis data support the downtime? Are data sources cited? How does the downtime value compare with downtimes for analogous systems?

3.2.2. Operational Availability Attribute.

3.2.2.1. Is there evidence of a comprehensive analysis of the system and its planned use, including the planned operating environment, operating tempo, reliability and maintenance concepts, and supply chain solutions leading to the determination of the value? Are the analyses documented?

3.2.2.2. Are definitions provided for failures, mission-critical systems, and criteria for counting assets as “up” or “down?” Are the values for failure rates supported by analysis?

3.2.2.3. Is scheduled downtime that affects the CONOPS identified and included? Does the analysis package support the downtime? Are data sources cited? How does the downtime value compare with that experienced by analogous systems?

3.2.2.4. Is downtime caused by failure addressed? Are the values used for failure rates supported by the analysis? Is there a definition established for failure?

3.2.2.5. For complex systems and systems of systems, is the operational availability defined at the appropriate system level?

3.2.3. Reliability Attribute.

3.2.3.1. Has the reliability metric been established at the system level? Is it traceable to the original capability requirements, or other performance agreement?

3.2.3.2. Does the analysis clearly provide criteria for defining relevant failure?

3.2.3.3. Does the analysis clearly define how time intervals will be measured?

3.2.3.4. Does the analysis identify sources of baseline reliability data and any models being used? Is the proposed value consistent with comparable systems? Are sources of data and processes to track reliability across the lifecycle identified?

3.2.3.5. Is the reliability value consistent with the intended operational use of the system (i.e., the CONOPS), and/or OMS/MP?

3.2.3.6. Is the reliability value consistent with the sustainment approach as presented in the operational availability metric?

3.2.3.7. Is the reliability value improved relative to fielded or analogous systems? If lower reliability is proposed, what improvements are gained in other areas to make the trade-off valuable to the warfighter?

3.2.3.8. For single-shot systems and systems for which units of measure other than time are used as the basis for measuring reliability, does the analysis package clearly define the units, method of measuring or counting, and the associated rationale?

3.2.4. Maintainability Attribute.

3.2.4.1. Has the maintainability metric been established at the system level? Is it traceable to the original capability requirements, or other performance attributes?

3.2.4.2. Is the maintainability metric linked to the RAM-C analysis? Does the analysis balance the maintainability metric against the reliability and O&S cost metrics?

3.2.4.3. Is the maintainability metric improved relative to fielded or analogous systems? If a higher repair/turn-around time is required, what improvements are gained in the other areas to make the trade-off valuable to the warfighter?

3.2.4.4. Are the maintainability attributes derived from or consistent with the CONOPS and expected operational environment?

3.2.4.5. Are the planned operational conditions and limitation for maintenance understood and incorporated into the design?

3.2.4.6. Will the maintenance requirements of the system cause additional training, manpower, support equipment, or infrastructure changes?

3.2.4.7. Does any of the planned use of Interim Contract Support (ICS) or Contractor Logistics Support (CLS) match operational or Service limitations on contractors in the battlefield?

3.2.4.8. Does the system design lend itself to easily accessible maintenance for operational or depot capabilities?

3.2.4.9. Does the mean time to repair (MTTR) definition assumptions included parts, personnel and support equipment in place?

3.2.4.10. Does the mean down time (MDT) definition include depot maintenance or is it focused on operational maintenance?

3.2.4.11. Is there evidence that maintainability attributes consider both organizational level system requirements (MTTR & MDT) as well as supply chain attributes (supply response times, higher echelon repair turnaround times, etc.)?

3.2.5. O&S Cost Attribute.

3.2.5.1. Has the O&S cost goal/constraint been defined for the system?

3.2.5.2. Does the analysis use the CAPE O&S cost element structure? Are there costs included in the O&S Cost system attribute that fall outside of the CAPE O&S cost element structure? If so, have those costs been explained in sufficient detail?

3.2.5.3. Is the documentation for the O&S cost estimate of the objective value supplied and available in the KM/DS system? If so, is it to an appropriate level of detail to adequately explain the estimate values?

3.2.5.4. Is the cost estimate consistent with the assumptions and conditions being used for materiel availability and reliability?

3.2.5.5. Is the O&S cost attribute traceable to the original capability requirements, or agreement with the warfighter?

3.2.5.6. Are all required costs included, regardless of funding source or management control?

3.2.5.7. Were applicable environmental issues considered in the development of the O&S cost estimate?

3.2.5.8. Is the O&S Cost system attribute data consistent with the capability solution's lifecycle cost estimate (LCCE), Cost Analysis Requirements Data (CARD) and/or the CAPE independent cost estimate (ICE) if available for comparison?

3.2.5.9. Is the threshold value for the O&S Cost system attribute calculated as 10 percent higher than the objective value?

3.2.5.10. Has the annual cost of a system (or systems for munitions and networks) been provided as part of the rationale?

3.2.6. Are sources of data, information systems, and processes identified to track the Sustainment performance attribute and its supporting attributes across the lifecycle? What models are used to establish and track the Sustainment performance attribute and supporting attributes?

3.2.7. Other logistics attributes.

3.2.7.1. Is there evidence of analysis of the system and its planned use, including the operating environment, operating tempo, reliability, maintenance concepts, and supply chain solutions (logistics and administrative downtime) leading to the determination of each attribute's value? Are the analyses documented?

3.2.7.2. Are definitions for each attribute's value provided? Are they supported by analysis and are they testable?

3.2.7.3. Are information systems for sources of data and processes to track each attribute's metric or value across the lifecycle identified? Are there models or simulations available that establish or track each attribute?

3.2.7.4. Does the attribute require discrete funding and is that requirement included in the O&S Cost APA, LCCE, CARD, and/or CAPE ICE?

3.2.7.5. Is the administrative and logistics downtime associated with failures addressed (e.g., recovery time, diagnostics time, movement of maintenance teams to the work site, etc.)?

3.2.7.6. Has the Administrative and Logistics Downtime (ALDT) been established by the Program Manager in the PM's RAM-C report for use in technical feasibility, maintainability and availability calculations?

3.2.8. Other performance attributes (KPPs, KSAs, or APAs)

3.2.8.1. Do any of the other performance attributes (KPPs, KSAs, or APAs) require specific or discrete logistics support or affect the Sustainment KPP or its supporting KSAs or APAs?

3.2.8.2. Are there logistics information systems for sources of data and processes to track the performance attributes (KPPs, KSAs, or APAs) that impact logistics support?

3.3. Endorsement Documentation: Upon successfully endorsement of the Sustainment KPP, the Logistics Chair will provide the Sponsor with an endorsement memorandum that will be included with the JCIDS document and maintained within the KM/DS system.

	Distinguishing Characteristics	Materiel Availability	Operational Availability	Reliability[1]
Ship Platforms	Naval vessels with multiple missions and multiple large or complex systems. Planned down time.	Availability of the entire population of systems for tasking when a ship is not in a planned maintenance availability or unavailable due to CASREP 4 failure.	Percentage of time an operationally deployed ship is not in a CASREP 4 state over a given operating period.	• Mission Reliability = (operating hours/mission failures) • Logistics Reliability = (operating hours/logistics demands)
Aircraft Platforms	Aviation programs with integrated systems, multiple missions.	Number of available aircraft/Total aircraft inventory.	Uptime/Total Time.	• Mission Reliability = (flight hours/mission failures) (e.g., operational mission failure) • Logistics Reliability = (flight hours/logistics demands)
Ground Vehicles or Mobile Ground Systems	Wheeled or tracked platforms, either towed or self-propelled.	Number of available vehicles/Total vehicle inventory.	Uptime/Total Time.	• Mission Reliability = (hours or miles/mission failures) (e.g., system abort) • Logistics Reliability = (hours or miles/logistics demands)
Weapons[2]	Single use (e.g., air-launched weapons, missiles).	Number of available weapons/total weapon inventory. Repairable devices must include the pipeline or depot inventory.	Number of times system is available/ number of times system is required.	• Mission Reliability = (successful launches/total launch attempts) • Logistics Reliability = (operating hours/logistics demands)
Satellite Systems (including hosted payloads)[3, 4]	Sub-types include an individual, single purpose satellite, a constellation of two or more satellites, and hosted payloads that share certain satellite infrastructure functions.	Unless unique circumstances exist (e.g., periodic software uploads), once the system is on-orbit Materiel Availability is not applicable.	Functional Availability: Probability of satisfying the minimum level of performance for a specific mission as a function of time,	• Mission Reliability: The probability of a satellite to perform a required function under stated conditions for a specified period • Logistics Reliability = N/A

	Distinguishing Characteristics	Materiel Availability	Operational Availability	Reliability[1]
			typically expressed as a probability of success.	
Modification Programs[5]	Replacement or upgrade of existing systems or subsystems.	Determine applicability dependent on existing system type.	Up Time/Total Time.	• Mission Reliability = (operating hours/mission failures) • Logistics Reliability = (operating hours/logistics demands)
Subsystems	Clearly defined interfaces, installed in host platform.	Number of available subsystems/Total subsystem inventory.	Up Time/Total Time.	• Mission Reliability = (operating hours/mission failures) • Logistics Reliability = (operating hours/logistics demands)
System of Systems or Unmanned Systems[6]	Collection of distinct system elements that create a combined mission capability. (Define Am, Ao, Reliability parameters for each system)	Number of available systems/total system inventory.	Uptime/Total Time.	• Mission Reliability = (operating hours/mission failures) • Logistics Reliability = (operating hours/logistics demands)
Automated Information Systems (AIS)	A system of computer hardware, computer software, data or telecommunications that performs functions such as collecting, processing, storing, transmitting, and displaying information.[7]	Unless unique circumstances exist, materiel availability is not applicable. These systems operate as a single collective system.	Uptime/Total Operating Time.[8, 9]	• Mission Reliability = N/A • Logistics Reliability = N/A

Notes:

[1] More than one reliability metric may be specified as a KSA and/or an APA as appropriate. Mission Reliability is the measure of the ability of an item to perform its required function for the duration of a specified mission profile. Logistics Reliability is the measure of the ability of an item to operate without placing a demand on the logistics support structure for repair or adjustment (All system failures regardless of impact on the mission).

[2] Weapons which are active/on during captive carry (aircraft platforms) or significant on time (ship and ground launched systems) should consider a KSA for logistics reliability.

[3] Hosted payloads: Functional Availability may also be a function of the reliability of shared infrastructure depending on the CONOPS.

[4] Constellation: Functional Availability is a function of the reliability of the necessary minimum of satellites and the mission success criteria.

[5] Modification Systems should consider the existing system requirements structure.

[6] In the case for Unmanned Aerial Systems, the air vehicle would measure reliability in flight hours versus operating time.

[7] Excluded are computer resources, both hardware and software, that are an integral part of a weapon or weapon system.

[8] Operating time is the time the system is in use (executing) IAW the OMS/MP or mission thread. Different KPP values may be assigned for the mission threads if appropriate.

[9] Mean restore time is an appropriate metric to support the availability KPP for AIS. Detection and isolation metrics also should be established to support the mean restore time.

Figure B- 23: Recommended Sustainment Metrics

ANNEX E TO APPENDIX G TO ENCLOSURE B
ENERGY KPP GUIDE

1. Overview.

1.1. Purpose: This guide assists Sponsors in the development of the Energy KPP values that affordably manage energy demand and related energy logistics and security risks without degrading mission effectiveness of the capability solution. While this guide does not prescribe an exact analytical methodology to establish Energy KPP attributes and values, it provides factors to be considered to ensure the rationale being provided meets the rigor needed for critical review.

1.1.1. The Energy KPP (one of four mandatory KPPs) differs from other KPPs in several ways:

1.1.1.1. Fuel delivery logistics (tanker aircraft, oilers, and fuel trucks) have a uniquely large presence in the total force structure and in the battlespace.

1.1.1.2. Fuel, in the large volumes U.S. forces demand it, and, in the timeframe when new systems will come into the force, may become less readily available for procurement in proximity to where it is required for operations.

1.1.1.3. The Energy KPP does not focus directly on energy-related costs, but rather on mission effectiveness within the context of mission and threat.

1.2. Applicability. The Energy KPP is applicable in CDDs that specify capabilities that use operational energy or consume energy to sustain performance over scenario timelines.

1.3. Proponent. The Energy KPP proponent is the J-4/Engineering Division (J-4/ED), with analytical support from the Office of the Deputy Assistant Secretary of Defense for Operational Energy (DASD(OE)). For questions, contact J-4/ED at (703) 697-4443.

2. Energy KPP Content Guide.

2.1. Operational Implications of Energy.

2.1.1. The proliferation and improvement of adversary capabilities to threaten or deny lines of communication, coupled with growing fuel and electrical power demand across the joint force, mean operational limitations on energy logistics must be included in the trade space for any new system that demands energy in operations. Further, there is an inherent opportunity cost to the Department and force structure in allowing logistics support, particularly energy-related delivery, to grow without analyzing the value of reducing the demand for their support. The same consideration applies to force protection for those logistics forces.

2.1.2. The Energy KPP is intended to ensure combat capability of the force by balancing the energy performance of systems and the provisioning of energy to

sustain required systems/forces by the operational commander in relevant threat environments. Energy performance is a key component of system and unit performance and relates to the required energy consumption needed to perform functions or tasks in operational modes, mission profiles/durations, and environmental conditions.

2.1.3. The Energy KPP includes, but is not limited to, considerations for optimizing fuel and electric power demand in capability solutions, in the context of the logistical supply of energy to the warfighter, as it directly affects the demand on the force to provide and protect critical energy supplies. The Energy KPP includes both fuel and electric power demand considerations in systems, including those for operating "off grid" for extended periods when necessary, consistent with SSA products.

2.1.4. In cases where energy demand reduction is impractical or insufficient to align with projected energy supply, complementary DOTmLPF-P changes to the energy supply chain and associated logistics capability solutions must be addressed in the document to accommodate the increased energy demands and satisfy the Energy KPP.

2.2. Energy Supportability Analysis.

2.2.1. General Considerations. Analysis of the system's use of energy to accomplish mission requirements forms the basis of all energy performance attributes and the Energy KPP. This analysis serves to expose energy demand and supply relationships and thereby influence system design considerations and KPP development. The Sponsor shall upload associated Energy Supportability Analysis document to KM/DS together with each capability requirements document designated as a JPR, unless the Energy KPP Proponent has approved a waiver.

2.2.1.1. Energy performance is a key component of system and unit performance and relates to the required energy to perform certain functions or tasks in operational modes, mission profiles, and environmental conditions. Energy KPP values establish the energy performance threshold and objective values for a capability solution, and are derived from the operational requirements of the system, scenario-based assumptions for its operational use, and the planned logistical and force protection support to sustain it.

2.2.1.2. Initial analysis should use independent energy analysis or the capabilities-based assessment to optimize future system effectiveness. Identifying energy performance considerations "up front" enables the acquisition and requirements communities to make decisions that balance energy demand and energy supply with other elements of performance, enabling optimal capability solutions for the warfighter.

2.2.1.3. The analysis is to be framed by explicit assumptions such as realistic threat and operations tempo, consistent with the DIA- or Service-approved threat products used for the threat summary section of the capability requirements document.

2.2.1.3.1. The analysis underpinning the Energy KPP must be scenario-based, must use the logistics assets programmed for the future force, and must use the most stressing scenario, from an energy demand perspective, outlined during development of the AoA or similar study. The analysis must be derived from SSA products that include not only operation of the system in question but also the energy-related logistics and required force protection needed in contested operational domains, including considerations for operating "off grid" for extended periods when necessary. All SSA products used by the program for this analysis must be of sufficient duration (multiple days to weeks) to demonstrate the effect of realistic opponent effects on the U.S. and/or coalition logistics force. Such analysis is required because kinetic and non-kinetic capabilities to potentially counter logistics are proliferating and because operational experience has shown the inherent vulnerability and opportunity cost of employing and protecting large logistics forces in contested domains.

2.2.1.3.2. The scenario analyses, therefore, must include the required logistics forces as well as realistic threats and disruptions to those logistics. The scenario must account for availability of logistics assets, non-hostile attrition (including reliability), and attrition due to red action against blue logistics systems. Some of the same scenario-based analysis used for the CONOPS or AoA may be leveraged to set Energy KPP thresholds and objectives. This interplay of combat and support forces, based on DoD Component and joint planning factors and SSA products, will help identify the required Energy KPP attributes needed to be mission capable. It is from these operational metrics that technical system metrics can be established.

2.2.2. Three-part methodology.

2.2.2.1. The first part of the methodology is to analyze the energy supply capacity available to the entire unit of maneuver, considering other consumers of the same energy logistics. Energy supply capacity is not a single number, but an accounting of the future capacity of the supply chain to deliver energy to the future unit of maneuver over time during the scenario.

2.2.2.1.1. The analysis exposes the energy demands of the system during its mission profile in the interval between refueling/recharging events. For all systems, the interval between refueling/recharging events is determined by the tempo and availability of refueling assets as modeled in the context of the most stressing validated operational level scenario.

2.2.2.1.2. The analysis addresses the ability to transport, distribute, store, and protect the energy supply within the scenario. Specifically, the analysis must consider:

2.2.2.1.2.1. Duration of the mission profile for the platform under consideration, using the most stressful scenario from an energy demand perspective.

2.2.2.1.2.2. Force Structure (including projected future force structure of scenario and associated support systems across the full unit of maneuver).

2.2.2.1.2.3. CONOPS and TTPs.

2.2.2.1.2.4. Adversary threat to energy logistics assets, and required force protection assets as mitigation.

2.2.2.2. The second part of the methodology involves looking at the energy demands of the platform, the unit of maneuver, and other consumers of the same energy logistics. This analysis examines the desired performance of the system and its impact on energy sources, either as a receiver (drawing energy from other systems) or as a provider (supplying energy to other systems). Understanding provider/receiver energy relationships and integration requirements of a system is important to scoping the supportability analysis and for refining the energy performance attributes in the operational context, as outlined in with Figure B-24.

2.2.2.2.1. The system must be considered as a potential end-user; this means that its propulsive, heating and cooling, sensing and firing systems all bear on the energy consumed by the platform as it transports itself and its payload and defends itself.

2.2.2.2.2. The system must also be potentially considered as one node in an energy distribution network, in which the platform may function as an energy provider to receiver systems that are dependent on the platform's store of energy. These potential receiver systems could broadly range from embarked weapons systems (i.e., LCACs, helicopters, aircraft, ground vehicles, etc.) to serviced weapon systems (i.e., refueled ships, aircraft underway or in-flight) as well as intrinsic energy demanding components such as radars which must necessarily draw their energy demand from the energy providing platform to complete their mission. The distinction between energy provider and receiver is important when determining how to apply the Energy KPP. Systems that must function as both may require an Energy KPP for each role.

2.2.2.2.3. For programs that seek to replace a subsystem, such as an engine upgrade or addition of a drag reduction device such as winglets to a legacy platform, the energy performance comparison can be stated as a percentage improvement over the legacy system. This comparison must be based on identical missions under identical threats. Testability can be simplified by specifying developmental test conditions under which the legacy subsystem performance is well documented.

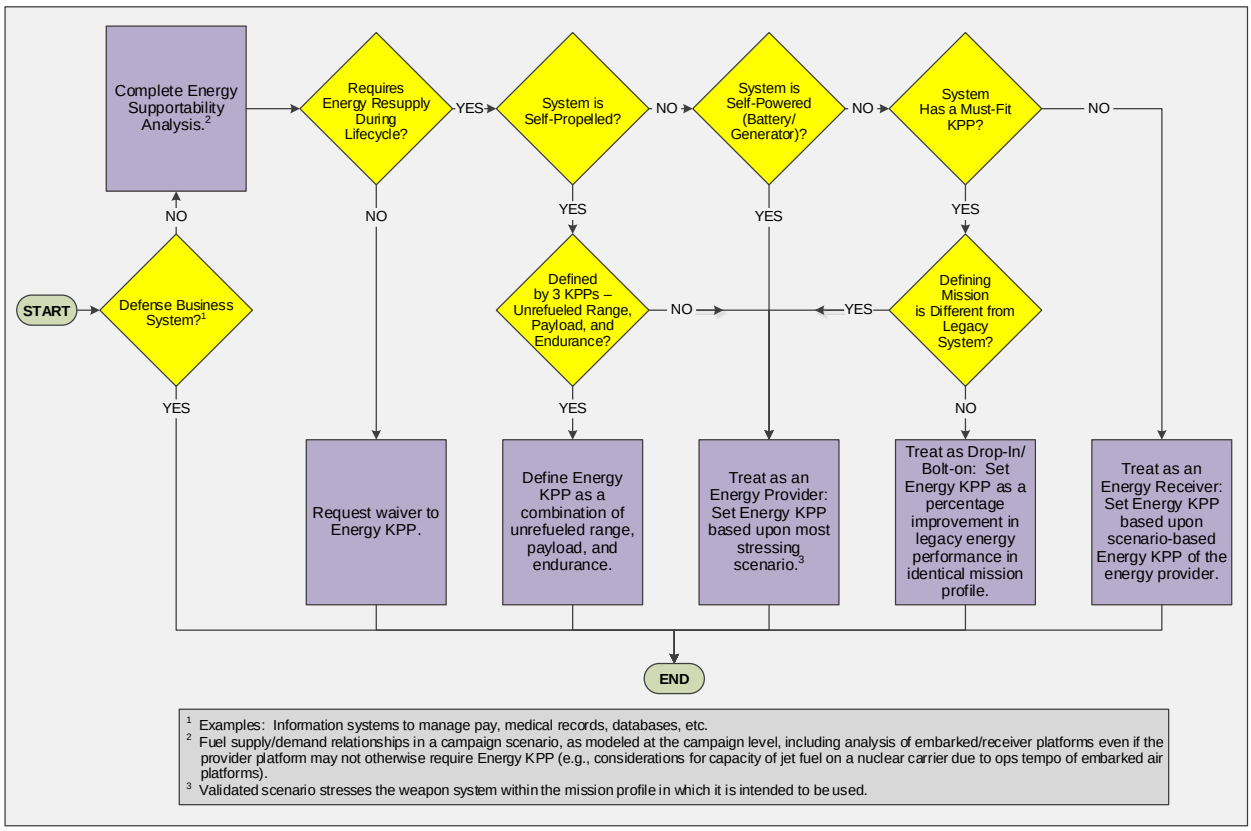

Figure B- 24: System Roles for the Energy KPP

2.2.2.3. The third part of the methodology is to analyze the difference, in the context of the scenario and the threat, between the capacity to supply energy and the energy demand. How this difference is addressed will assist in determining the key attributes to be included in the Energy KPP, and their associated threshold and objective values. The energy supportability analysis will ultimately identify energy performance attributes that directly affect the system's ability to perform its mission. In turn, these energy performance attributes, when related directly to the system's mission effectiveness parameters, will frame the system's Energy KPP attributes.

2.2.2.3.1. The design, technology, lifecycle cost, schedule, and quantity trades between each variable that affects energy demand on-board (powerplant, weight, drag, electrical load, etc.) can be used to derive the threshold and objective values for system energy performance.

2.2.2.3.2. A Sponsor may find that the required performance of the platform from step two above is not possible given current technological state of the art, the performance limits of a fielded platform being modified, or other limiting factors. When the fuel allocation for the weapon system is insufficient given the limitations of the scenario and the technology of the system, the Sponsor must find a means to correct the imbalance. This reinforces the need for a scenario-based analysis for the Energy KPP.

2.2.2.3.3. Sponsor options to balance a supply and demand may include decreasing consumption through greater platform efficiency, reducing the number of platforms in the unit of maneuver, increasing the capacity of the supply chain (i.e., increase logistics assets), changing the scheme of maneuver, or modifying CONOPS or TTPs. In cases where a platform consumes more energy than its predecessor consumes, or has no predecessor, a Sponsor must address complementary DOTmLPF-P change(s), including required associated resources needed to implement the changes, which accommodate the consumption increase above what the energy supply chain can provide.

2.2.2.3.4. Regardless of the approach, the Sponsor must balance the planned consumption of the unit of maneuver with the capacity of the supply chain providing energy to the unit of maneuver, considering other consumers of the same energy logistics. Increases in system energy consumption should be mitigated to the maximum extent practicable.

2.3. Energy Performance Attributes.

2.3.1. Energy performance attributes relate energy consumed by the system to the operational effect produced by that consumption. Those selected should be the most critical to the mission effectiveness of the system.

2.3.1.1. Provider Systems. Provider systems include any system that supplies energy to other systems. Sponsors of provider systems may consider potential energy performance attributes that include but are not limited to the following, in order to facilitate development of their Energy KPP:

2.3.1.1.1. Payload-ton-miles/gallon or Payload-ton-miles/kWh where payload weight and combat range are important to mission effectiveness

2.3.1.1.2. Payload-ft3-miles/gallon or Payload-ft3-miles/kWh where payload volume and combat range are important to mission effectiveness

2.3.1.1.3. Energy consumed (gallons, kWh) per unit of mission accomplished (e.g., square miles of ocean swept for mines at the required depth and level of effectiveness; required targets detected, tracked and engaged at specified range/conditions, etc.)

2.3.1.1.4. Energy (gallons, kWh) consumed between refueling events as the system and any receiver systems complete their most stressful, most energy-consuming mission profile

2.3.1.1.5. Energy capacity (gallons, kWh) supplied to receiver systems where the provider system is expected to be the sole source over a critical period of time

2.3.1.2. Receiver Systems. Receiver systems draw energy from their provider systems. Sponsors of receiver systems may consider potential energy performance attributes that include but are not limited to the following, in order to facilitate development of their Energy KPP:

2.3.1.2.1. Energy capacity (gallons, kWh) drawn from the provider over a critical period of time, where the provider is the sole energy source.

2.3.1.2.2. Energy consumed (gallons, kWh) per unit of mission accomplished (e.g., square miles of ocean swept for mines at the required level of effectiveness, required targets detected, tracked and engaged, etc.).

2.3.1.2.3. Peak power demand or maximum fuel delivery rate imposed by receiver systems on their energy provider, where surges of receiver system performance are important to mission effectiveness.

2.3.1.3. Drop-In/Bolt-On Systems or Sub Systems. For programs that seek to replace a powertrain component such as an engine in a legacy platform or add a drag reduction device such as winglets to a legacy platform, the energy performance comparison can be stated as a percentage improvement over the legacy system, with the comparison based upon identical mission profiles. Sponsors of systems that are being integrated into a legacy platform may consider potential energy performance attributes that include but are not limited to the following, in order to facilitate development of their Energy KPP:

2.3.1.3.1. Ratio of power transmitted to power supplied (kW:kW, HP:HP; can be expressed as percentage) where a subsystem is proposed as a drop-in/bolt-on replacement in a power train.

2.3.1.3.2. Drag reduction or propulsive effectiveness gain (decrease in gallons per ton-mile, percentage difference in range/payload or endurance) where a component affects cruise performance.

2.3.1.3.3. Thrust-specific or HP-specific fuel consumption improvement.

2.3.2. Relationship with other performance attributes. Performance attributes of the system or network that do not address both energy and performance are not considered energy performance attributes. For example, for a radar system the peak power demand that the radar imposes on its host ship/aircraft/vehicle in radar mission mode is an energy performance attribute. Likewise, the ratio of electrical energy the radar demands to the energy emitted from the radar antenna in mission mode is an energy performance attribute. However, the radar's detection range and discrimination accuracy by themselves are not considered energy attributes.

2.3.3. Testability. Selection of Energy KPP attributes should take into account any testability issues and be selected in a way that supports cost effective evaluation. For example, to demonstrate compliance with an attribute that relates energy demand to performance stated in terms of probability, the Sponsor must coordinate with the DOT&E community to determine the required combination of testing and parametric modeling.

3. Energy KPP Endorsement Guide. This guide provides procedures for the Logistics FCB Chair to review the Energy KPP during the staffing of JCIDS documents. On behalf of the Logistics FCB Chair, J-4/ED evaluates and endorses the Energy KPP in capability requirements documents, with analytical support from the Office of the DASD(OE). When responsibility to review and endorse the Energy KPP is assigned to the Sponsor IAW Enclosure A of this manual, the Sponsor may deviate from this endorsement guide. Any substantive changes to this guide will be coordinated with and approved by the DJ-4 or designee.

3.1. Review Process. J-4/ED, with support from the office of the ASD(OEPP), will review energy performance metrics for alignment with Energy KPP guidance provided in this annex.

3.1.1. J-4/ED receives, via the KM/DS systems, all JROC Interest or JCB Interest documents.

3.1.2. J-4/ED reviews and assesses the Energy KPP and recommends to the Joint Staff Gatekeeper whether the Energy KPP should be designated a JPR.

3.1.2.1. If designated a JPR then J-4/ED reviews and assesses the Energy KPP for compliance with the Energy KPP Content Guide.

3.1.3. J-4/ED reviews and coordinates with the office of the ASD(OEPP) for Energy KPP analysis.

3.1.4. J-4/ED consolidates and enters comments into the KM/DS system.

3.1.5. J-4/ED and the office of the ASD(OEPP) will provide representation to the JROC and subordinate boards for unresolved critical comments.

3.2. Review Criteria.

3.2.1. Energy Supportability Analysis.

3.2.1.1. Is there evidence of a comprehensive analysis of the system and its planned use, including the intended operating environment, operating tempo, and supply chain solutions/limitations leading to the determination of the Energy KPP attribute values?

3.2.1.2. Does the analysis present energy performance and mission effectiveness relationships?

3.2.1.3. Does the analysis identify the most critical attributes associated with the use, delivery, storage, or protection of energy that impact mission success?

3.2.1.4. Did the Sponsor provide the assumptions on which the analysis is based?

3.2.1.5. Does the analysis present energy supply/demand relationships?

3.2.2. Scope.

3.2.2.1. Are the CONOPS and/or OMS/MPs based on relevant situations derived from the approved scenario?

3.2.2.2. Do the energy performance attributes encompass critical energy-demanding activities the system must perform within the mission profile?

3.2.2.3. Do the threshold and objective values of the energy performance attributes enable operations at the required tempo and CONOPS given limitations on the energy supply in the operational area?

3.2.3. Relevance.

3.2.3.1. Do the energy performance attributes relate energy demand directly to a relevant combat performance issue?

3.2.3.2. Is there evidence of due diligence to determine threshold and objective values for energy performance attributes relevant to the state of technology?

3.2.4. Clarity.

3.2.4.1. Do the energy performance attributes directly relate to mission effectiveness by improving the system's energy performance?

3.2.4.2. Are the energy performance attributes expressed in commonly used terms and/or metrics?

3.2.5. Measurability.

3.2.5.1. Are the energy performance attributes quantified in metrics commonly tested in similar systems?

3.2.5.2. Can compliance with the energy performance attribute be demonstrated by a combination of test results and modeling acceptable to the DOT&E community?

3.3. Waiver Process.

3.3.1. Sponsors requesting relief from the Energy KPP, if designated as a JPR, must seek approval for a waiver through J-4/ED. Together with the waiver request, the Sponsor will provide the analysis supporting the assessment that the Energy KPP is not applicable.

3.3.1.1. Under waiver authority Sponsors may opt out of preparation of mandatory Energy KPP and ESA. Waiver is applicable for CDD when the balance of energy performance and the provision of energy to the system (fuel and electric energy) neither impacts operational research nor requires added protection of energy infrastructure or energy resources in the theater logistics supply chain.

3.3.1.2. Suggested waiver categories include the following: Information systems (software only); CONUS-only, Non-deployable, Space, Training systems; Energy source is self-contained or nuclear and system is not an "energy-provider" (e.g., expendable munitions); and permanent component

replacements where the electrical dependencies were evaluated via a Systems Engineering Plan (SEP).

3.3.2. J-4/ED, with assistance from the office of the ASD(OEPP), will review the request and the supporting documentation. J-4/ED will either approve the waiver or inform the Sponsor why the waiver was not approved.

3.3.3. Because the acquisition process deals with trade space and balancing cost, schedule, and performance, waivers must be carefully weighed. "The new platform doesn't use more energy than the old platform" is not a sufficient justification for a waiver. Without an Energy KPP, that energy limit could be "traded" for some other attribute. In this example, the threshold value of an Energy KPP attribute could be the same as the previous platform; the Sponsor is not spending money to be more energy efficient but the current energy efficiency cannot be traded away to improve some other performance attribute.

3.4. Endorsement Documentation. Upon successfully endorsement of the Energy KPP, the Logistics Chair will provide the Sponsor with an endorsement memorandum that will be included with the JCIDS document and maintained within the KM/DS system.

ANNEX F TO APPENDIX G TO ENCLOSURE B
DOTmLPF-P GUIDE

1. Overview. The DOTmLPF-P Guide is intended to ensure Sponsors adequately address non-materiel aspects of a capability during requirement definition and capability development.

1.1. Purpose. The purpose of the DOTmLPF-P content in capability requirements documents is to address non-materiel aspects of a capability recommendation. An ICD or DCR should describe non-materiel approaches that could provide a capability solution which closes or mitigates associated capability gaps. A CDD should describe non-materiel enablers to materiel capability solutions without which the materiel capability solution cannot be successfully fielded. DOTmLPF-P considerations pertain to both materiel and non-materiel solutions. While DOTmLPF-P considerations are readily apparent in non-materiel solutions, they are not readily apparent for materiel solutions where DOTmLPF-P considerations are needed to fully implement the materiel solution. In all of the above examples, DOTmLPF-P content should also describe the potential non-materiel changes necessary to implement the proposed recommendation(s).

1.2. Applicability. Sponsors must address all DOTmLPF-P considerations in capability requirements documents. In cases where one or more of the DOTmLPF-P considerations may not be applicable, the Sponsor shall state this in the document and explain why and coordinate with the proponent identified in paragraph 1.3 below to ensure that the DOTmLPF-P endorsement is not withheld due to missing information.

1.3. Proponent. The DOTmLPF-P proponent is the J-7/JIB, on behalf of the Joint Staff Director for Joint Force Development (DJ-7). For questions, please contact the J-7/JIB at (703) 692-0785, (703) 695-9124, (703) 695-5436, (703) 692-6294, (703) 697-8881 or js.pentagon.j7.mbx.jib-jcids@mail.smil.mil (SIPRNET).

1.4. Joint DOTmLPF-P FPOs. FPOs are division-sized subject matter expert organizations within the Joint Staff that are designated for each of the DOTmLPF-P considerations. Their role is to provide advice to Sponsors related to their functional area on all joint requirement documents and affected FCBs during the drafting and review of those documents. FPOs operate under a parent directorate and are not only subject matter experts in their relevant consideration of DOTmLPF-P, they understand the relationship of their consideration to the other DOTmLPF-P considerations and to the requirements process in general. FPOs will review all joint requirements documents during the requirements review process, and their comments will be included in their parent J-DIR vetting of the requirements document. FPOs also will send an information copy of their comments to the J-7/JIB for use by the J-7 in

preparing the DOTmLPF-P endorsement of the joint requirements document under consideration. The FPOs are listed in Figure B-25.

DOTmLPF-P Consideration	Functional Process Owner (FPO)	Associated Guidance/Processes
Joint Doctrine	JS/J-7/DDJED(DOC)	References [80]
Joint Organization	JS/J-8/DDRA(PBAD)	Reference [81]
Joint Training	JS/J-7/DDPMA(PPD)	Reference [82]
Joint Materiel	JS/J-8/DDRA(CAD)	N/A (Coordinate quantity changes with affected Sponsors)
Joint Leadership and Education	JS/J-7/DDJED(JPMED)	References [83] and [84]
Joint Personnel	JS/J-1/PRD	Reference [85]
Joint Facilities	JS/J-4/DDOL(M)	References [86], [87], and [88]
Joint Policy	JS/J-5/DDGP&P(SCS)	Reference [89]

Figure B- 25: DOTmLPF-P FPOs

2. DOTmLPF-P Content Guide. Implementation of changes to DOTmLPF-P validated in the JCIDS process may require coordination with other impacted organizations and processes. Sponsors are encouraged to coordinate proposed changes with impacted organizations during document development to facilitate timely staffing and validation. If no changes are required or recommended state so. Additionally, Sponsors will address all of the following DOTmLPF-P considerations in their requirements document:

2.1. Doctrine. The doctrine consideration of DOTmLPF-P consists of fundamental principles that guide the employment of U.S. military forces in coordinated action toward a common objective.

2.1.1. Identify the joint or service doctrine that is applicable.

2.1.2. If current doctrine is insufficient, explain why.

2.1.3. Identify the changes that would be needed in designated joint or service doctrine to describe how the recommended capability should be captured in doctrine. Identify the OPR(s) for any proposed doctrinal change.

2.1.4. Ensure, to the maximum extent possible that terms used in the document are IAW the DoD Dictionary for Military and Associated Terms, Reference [90], or if not, then fully define the new term in the glossary.

2.1.5. Ensure changes to doctrine are made IAW the process outlined in References [80] and any applicable Service doctrine process.

2.2. Organization. The organization DOTmLPF-P consideration pertains to a joint unit or element with varied functions enabled by a structure through which individuals cooperate systematically to accomplish a common mission and directly provide or support joint warfighting capabilities.

2.2.1. Identify if current organizational structures allow the capability to be used to its fullest potential.

2.2.2. If changes to organizational structures are an enabler to implementation of the capability or would allow greater efficiency or performance of the capability, outline the changes that are recommended or required.

2.2.3. If costs are associated with organizational changes, ensure that associated costs are captured in resource estimates.

2.2.4. Changes to organization must adhere to the process outlined in Reference [81] and any applicable Service organization process(es).

2.3. Training. The training DOTmLPF-P consideration pertains to training (including mission rehearsals) of individuals, units, and staffs using joint doctrine or tactics, techniques, and procedures to prepare joint forces or joint staffs to respond to strategic, operational, or tactical requirements considered necessary by the CCMDs to execute their assigned or anticipated missions.

2.3.1. Training must be properly addressed from the beginning of the acquisition process, integrated with the planning and materiel development, and updated throughout the capability solution's lifecycle. Non-materiel aspects of training are addressed in this section of the DOTmLPF-P content. Aspects of training that require performance attributes of the materiel capability solution may be addressed in a KPP, KSA, or APA.

2.3.2. Outline recommended and required training that will enable effective implementation and performance of the capability solution, including training considerations that address concerns documented in Reference [91] and characterized by Reference [92].

2.3.3. Training implications are considered in the CBA and the AoA or similar study, where training implications may drive projected lifecycle cost of the system or where training costs may be a discriminator between different alternatives pursued. Training not planned, adequately funded, and integrated early, has the potential to be a significant lifecycle cost driver for a program, or contribute to a lack of readiness when the system is fielded. This action ensures training and resourcing information is incorporated early in program planning, enables comparison of lifecycle cost, schedule, performance, and quantity, and facilitates development of an optimal solution providing greatest enhancement of user capabilities.

2.3.4. Changes to training must adhere to the process outlined in Reference [82] and any applicable Service training process(es).

2.3.5. Ensure costs associated with training are captured in resource estimates.

2.4. materiel. "materiel" items, systems, or equipment needed to support the required capability. Materiel refers to increased quantities, modifications, improvements, or alternate applications of existing materiel or the purchase of COTS/GOTS/NDI. The letter "m" in the acronym is usually lower case since Joint DCRs do not advocate new materiel development, but rather advocate increased quantities or alternate applications of existing materiel to include

COTS/GOTS/NDI. Sometimes referred to as “little m” materiel, the materiel DOTmLPF-P consideration is everything necessary to equip DoD forces to operate effectively. Materiel includes ships, tanks, self-propelled weapons, aircraft, related spares, repair parts, and support equipment, but excludes real property, installations, and utilities.

2.4.1. Identify any required fielded materiel as part of the capability solution or as an enabler to allow the capability solution to be used to its fullest potential. Fielded materiel may be leveraged in either their original capacity or in an adaptation or repurposing not originally envisioned.

2.4.2. If changes to fielded materiel are an enabler to implementation of the capability or would allow greater efficiency or performance of the capability, outline the changes that are recommended or required.

2.4.3. If costs are associated with additional quantities or repurposing of fielded materiel, ensure that associated costs are captured in resource estimates.

2.4.4. Identify any COTS/GOTS/NDI required as part of the capability solution or as an enabler to allow the capability solution to be used to its fullest potential.

2.4.5. If costs are associated with procuring COTS/GOTS/NDI ensure that associated costs are captured in resource estimates.

2.4.6. Changes to “little m” materiel must be coordinated with the affected Sponsors.

2.5. Leadership and education. The leadership and education DOTmLPF-P consideration consists of professional development of joint leaders that is the product of a learning continuum that comprises training, experience, education, and self-improvement. The role of joint professional military education (JPME), as it is with non-joint professional military education (PME), is to provide the education needed to complement training, experience, and self-improvement to produce the most professionally competent individuals possible.

2.5.1. Identify if current leadership and education allows the capability to be used to its fullest potential.

2.5.2. If changes to leadership and education are an enabler to implementation of the capability or would allow greater efficiency or performance of the capability, outline the changes that are recommended or required.

2.5.3. If costs are associated with leadership and education changes, ensure that associated costs are captured in resource estimates.

2.5.4. Recommend changes to other (non-JPME) education programs that will focus on ensuring personnel are capable of fully implementing the capability solution.

2.5.5. Changes to leadership and education must adhere to the processes outlined in References [83] and [84], and to any applicable Service leadership and education process(es).

2.6. Personnel. The personnel DOTmLPF-P consideration ensures that qualified personnel exist to support joint capability requirements. The DOTmLPF-P personnel function should not be confused with the organization function. The number or quantity of personnel is a function of organization, while the quality, type, or skills of personnel is considered in the personnel function.

2.6.1. Identify if current manning (type of personnel) allows the capability to be used to its fullest potential.

2.6.2. If changes to manning are an enabler to implementation of the capability or would allow greater efficiency or performance of the capability, outline the changes that are recommended or required.

2.6.3. If costs are associated with manning changes, ensure that associated costs are captured in resource estimates.

2.6.4. Changes to personnel must adhere to the process outlined in Reference [85] and any applicable Service personnel process(es).

2.7. Facilities. The facilities DOTmLPF-P consideration pertains to real property consisting of one or more of the following: buildings, structures, ranges, utility systems, associated roads and other pavements, and underlying land. Key facilities are defined as command installations and industrial facilities of primary importance to the support of military operations or military production programs.

2.7.1. Identify if current facilities allow the capability to be used to its fullest potential.

2.7.2. If changes to facilities are an enabler to implementation of the capability or would allow greater efficiency or performance of the capability, outline the changes that are recommended or required.

2.7.3. If costs are associated with facility changes, ensure that associated costs are captured in resource estimates.

2.7.4. Changes to facilities must adhere to the processes outlined in References [86], [87], and [88], and any applicable Service MILCON processes.

2.8. Policy. The policy DOTmLPF-P consideration consists of any DoD, interagency or international policy issues that may impact effective implementation of changes in the other DOTmLPF-P considerations.

2.8.1. Identify if current policy allows the capability to be used to its fullest potential.

2.8.2. If changes to policy are an enabler to implementation of the capability or would allow greater efficiency or performance of the capability, outline the changes that are recommended or required.

2.8.3. Changes to policy must adhere to the process outlined in Reference [89] and any applicable Service policy processes.

3. DOTmLPF-P Endorsement Guide. This guide provides procedures for the J-7 and DOTmLPF-P stakeholder organizations to review issues, ensure all appropriate DOTmLPF-P considerations are addressed in capability requirements documents, and develop the DOTmLPF-P endorsement as part of document staffing. When responsibility to review and endorse DOTmLPF-P is assigned to the Sponsor IAW Enclosure A of this manual, the Sponsor may deviate from this endorsement guide. Any substantive changes to this guide will be coordinated with and approved by the DJ-7 or designee.

3.1. Review Process.

3.1.1. J-7/JIB reviews JCIDS documents for DOTmLPF-P issues with JSDs of JROC Interest, JCB Interest. J-7/JIB may also review other JCIDS documents when requested by J-8/DDRCD or the Sponsor. As DOTmLPF-P covers a broad range of topics, DOTmLPF-P FPOs listed in Figure B-25 will coordinate with J-7/JIB:

3.1.2. FPOs will provide J-7/JIB with concur/non-concur (with reason and recommended solution) for the DOTmLPF-P consideration. FPOs will insure up-to-date POC information is provided to J-7/JIB.

3.1.3. USD(P&R) will coordinate with Joint Staff J-7 JIB on DOTmLPF-P endorsements (ACAT I – programs only).

3.1.4. DOTmLPF-P Endorsement reviews will focus on:

3.1.4.1. Non-materiel approaches that address capability requirements identified in ICDs or DCRs, and eliminates or mitigates associated capability gaps.

3.1.4.2. Non-materiel enablers identified in CDDs that are associated with materiel capability solutions, without which the materiel capability solution cannot be successfully fielded.

3.2. Review Criteria.

3.2.1. J-7/JIB will use the content guide in this annex as the basis for the DOTmLPF-P review. Content not in compliance with this guidance shall be updated to the satisfaction of the FPOs identified in Figure B-25 before the J-7 will issue a DOTmLPF-P Endorsement.

3.2.2. The DOTmLPF-P Endorsement is based on review of the information provided in the JCIDS document and accomplishes the following:

3.2.2.1. Ensures non-materiel solutions and non-materiel aspects of materiel solutions are fully considered and documented or that the Sponsor provides justification regarding recommendation for their exclusion.

3.2.2.2. Develops recommended revisions to the document language to reduce or eliminate identified concerns.

3.3. Endorsement Documentation.

3.3.1. J-7/JIB will submit to the DJ-7 or designee a recommendation to grant or withhold the endorsement. Once determination is made, a signed endorsement memorandum will be uploaded to the KM/DS system.

3.3.2. If the DOTmLPF-P Endorsement is withheld, suggested changes and/or rationale will be included with the memorandum.

ANNEX G TO APPENDIX G TO ENCLOSURE B
INTELLIGENCE SUPPORTABILITY GUIDE

1. Overview.

1.1. Purpose. The objectives of this guide are to ensure that capability solutions are developed in the context of applicable adversary threat capabilities, that intelligence requirements have been identified and documented at the earliest possible point, and that all likely intelligence support requirements and shortfalls (if applicable) have been assessed for availability, suitability, and sufficiency.

1.1.1. The scope of the intelligence certification shall include the entire program or capability solution's lifecycle. Intelligence certification shall seek to:

1.1.1.1. Ensure Sponsors incorporate the most current, applicable intelligence information, and analysis into their capability development efforts.

1.1.1.2. Ensure that national and defense intelligence architectures remain capable of supporting future warfighting by identifying and assessing possible intelligence support requirement shortfalls created by programs and capabilities being reviewed. Programs that send, produce and/or receive intelligence data and/or services will conform to mandated standards cited in the DoD IT Standards Registry (DISR) and identified by the Functional Managers.

1.1.1.3. Preclude fielding capabilities, systems, or programs that are unsupportable by the national and defense intelligence communities.

1.2. Applicability. Intelligence certification including the DIA/TLA threat approval, IMD evaluation, and when applicable, the DIA Directorate for Operations Office of Counterintelligence (DO/OCI) protection threat review and threat production validation, is required for all capability requirements documents assigned a JSD of JROC Interest or JCB Interest.

1.2.1. Intelligence Supportability Shortfalls. It is possible that the Intelligence Community (IC) cannot support a capability solution's intelligence support requirements, or that a capability solution may create an intelligence shortfall. The risk of an intelligence shortfall is a central concern in the intelligence supportability assessment and certification process. Sponsors are required to provide sufficient information, and to perform adequate analysis, to enable reviewers to assess and identify intelligence support requirements and shortfalls.

1.2.2. Intelligence Certification will be granted for capability requirements documents that fully articulate threat and intelligence support requirements. Conditional intelligence certification will be granted for capability requirements documents that do not fully articulate intelligence support requirements, but

the Sponsor has agreed to address requirements within the appropriate time period as documented in the conditional intelligence certification memorandum. Capability requirements that meet intelligence supportability requirements within the specified time will be granted full certification. Those capabilities that do not meet intelligence supportability requirements will be reviewed and an extension to the conditional certification, if warranted, will be granted. The intelligence certification, full or conditional, will not be granted for capability requirements documents that have not received threat approval from the DIA.

1.3. Proponent. The proponent for the threat assessment, intelligence supportability, and the intelligence certification process is the J-283/IRCO on behalf of the Joint Staff Directorate for Intelligence (JS/J-2). For questions, contact J-283/IRCO at (757) 836-7030.

2. Intelligence Supportability Content Guide.

2.1. The information below provides guidance on drafting intelligence supportability content in capability requirements documents and serves as a reference to reviewers during the intelligence certification review process.

2.1.1. Sponsors must identify and explain known or anticipated intelligence support requirements and shortfalls that may result from the program, across the capability solution's entire projected lifecycle. This includes projected requirements for all intelligence data or information (collection requirements/parameters, analytical products, foundational geospatial intelligence (GEOINT) products including topographic maps, aeronautical and maritime Safety of Navigation (SoN) charts and data sets, etc.), infrastructure (intelligence systems, processes, etc.), and/or resources (intelligence funding, personnel, etc.). Sponsors must also include qualitative and/or quantitative attributes for each intelligence support requirement.

2.1.2. The Threat Summary paragraph in an ICD, and the Threat Summary and Intelligence Supportability paragraphs in CDDs are the primary intelligence-focused paragraphs in capability requirements documents. Intelligence support requirements and/or threats applicable to a capability solution may change over time. Understanding and specifying intelligence support requirements or shortfalls will become more refined as the capability requirements document progresses from ICD to CDD, as required.

2.2. Threat Summary. The intent of the Threat Summary paragraph is to ensure the capability requirement and associated capability gaps are based upon consistent threat environment information and references. All acquisition programs or capabilities that are expected to operate in a threat environment (lethal or non-lethal) must be developed IAW the most current DIA- or Service-approved threat products. Significant changes to current threats or the emergence of new threats, near-term or projected, associated with validated capability requirements and the development of related capability solutions may change the development of future capability solutions.

The applicable system and protection threat information must be continually updated to account for threats throughout the capability solution's projected lifecycle, IAW DIA- and Service-approved threat products. Sponsors shall also account for protection threats to RDT&E, production, and O&M resulting from technology transfer, espionage, and other adversarial collection efforts.

2.2.1. Threat assessment shall begin with identifying all anticipated capabilities that adversaries might employ against the capability being reviewed. The identified operational tasks, conditions, and standards should then be submitted to DIA to enable production of applicable Threat Modules, which identify projected adversary threat capabilities, including scientific and technological developments as well as reverse-engineering capabilities, which may affect a program or capability's design or implementation. DIA/TLA will assist Sponsors with incorporating adversary capabilities in the development of initial and successor capability requirements documents.

2.2.2. When addressing the Operational Threat Environment, Sponsors must describe the threat capabilities, threat tactics, and adversary doctrine that are drivers for the capability development.

2.2.3. Supporting threat references shall be cited in the Threat Summary.

2.2.4. CIPs.

2.2.4.1. CIPs (IAW Reference [35]) are defined as a threat capability or threshold established collaboratively by the requirements sponsor and the component capability developer, changes to which could critically impact the effectiveness and survivability of the proposed system.

2.2.4.2. CIPs will be included for capabilities in development that are determined to be threat-sensitive. Sponsors should coordinate with DIA during the development of the requirement to determine whether the capability is threat-sensitive and/or if CIPs are required.

2.2.4.3. DIA/TLA will evaluate the program threat summary, supporting documentation, and the performance attributes that are potentially threat dependent. If DIA/TLA determines that a CIP is warranted, they will submit a comment and supporting rationale via a CRM during JCIDS staffing for Sponsor adjudication. Such comment should be sufficient cause to initiate discussion between the Sponsor, Program Office, and the IC to identify an approved existing CIP or develop a new CIP to meet capability requirements. Concurrently, the Sponsor should request guidance from the Lead FCB for determination as to whether a CIP will be required before the program proceeds in staffing. Development and/or identification of a CIP will proceed based upon the Lead FCB determination.

2.2.4.4. If a CIP is required, the threat validation authority (DIA or Service, as appropriate) will approve the CIP and the Sponsor will ensure the CIP is submitted via the Community On-Line Intelligence System for End Users and Managers (COLISEUM). Sponsors will include the identification of the CIP and

the approval authority or cite the approval of the Lead FCB if a CIP is determined not to be required.

2.2.4.4.1. Intelligence certification will be withheld for new or revised programs that do not include a CIP in the JCIDS document during FCB Draft review. This would include programs that proceeded to the next Milestone in development that did not include a CIP in prior phases of development.

2.2.4.5. Reference to the CIP shall be included in the Threat Summary for ICDs, and CDDs citing the COLISEUM production requirement number, the DAMIR long name (DAMIR short name), CIP number, and threat topic.

2.2.4.6. A brief description of the relationship between a CIP and a supported KPP, and the potential impact if the CIP is breached, shall be included in Section 5 for CDDs. Sponsors should remain cognizant of potential classification changes associated with describing impacts caused by CIP breaches.

2.3. ICD Content. In addition to the requirements for Threat Summary and CIP information described, Sponsors must identify the intelligence support categories, when known, applicable to the capability described below in the Capability Requirements and Gaps/Overlays section in ICDs. Include a description of the intelligence support requirements, resources, or other programs necessary to enable each capability, and any current or projected gaps or shortfalls in intelligence support related to a category.

2.4. CDD Content. The intent of the intelligence supportability paragraph is to identify and assess all intelligence support requirements, and anticipated shortfalls, throughout the capability solution's lifecycle in one, comprehensive section of the CDD. In drafting the Intelligence Supportability paragraph of CDDs, Sponsors must address the following for each intelligence support category:

2.4.1. Identify the capability solution's current and programmed requirements for intelligence support.

2.4.2. In coordination with the capability's intelligence support personnel, assess the IC's ability to satisfy the identified requirements, including statements as to whether the required support will be available and sufficient throughout a given capability solution's lifecycle, not just for a portion of the lifecycle.

2.4.3. Identify any assessed or potential intelligence support shortfalls that result from, or may result from, the development, testing, operations, and/or the sustainment of the capability solution. Emphasis is placed on shortfalls that could affect or delay development, testing, or fielding the capability solution, or those shortfalls that may degrade the operational effectiveness or sustainment of the capability solution. Sponsors must also consider and address the cause of these shortfalls (such as technological capability shortfalls, undefined common intelligence data/metadata standards,

scheduling problems, or funding issues) and, if possible, estimate the magnitude of the shortfall in terms of scheduling delays, vulnerability, materiel, resources, training, manpower, and any other relevant criteria. In addition, address how applicable shortfalls may impact operational security or vulnerability to espionage during any point of the lifecycle. Note that information related to intelligence shortfalls may be, or may become, classified information when associated with a shortfall; therefore, Sponsors must ensure that this section of the document is marked accordingly.

2.4.4. Describe and discuss all possible solutions for identified shortfalls. Include key issues that must be resolved concerning each shortfall. Provide a plan to address such shortfalls, and a schedule or deadline to remedy each shortfall. If the solution lies outside the control of the program office, or is deemed to be unobtainable, provide a recommendation on how to address the shortfall, and identify the organization with the authority and responsibility to address the shortfall.

2.5. Other CDD paragraphs may also need to consider intelligence support or integration concepts; the intelligence supportability paragraph must be consistent with the Operational Context, Capability Discussion, Performance attributes (KPPs, KSAs, APAs), and DOTmLPF-P sections of the capability requirements document. While the content of the intelligence supportability paragraph must be developed in light of the several considerations above, and formatted per the example below, Sponsors must also:

2.5.1. Consider and address what, if any, DOTmLPF-P changes are needed to address support requirements if the capability solution is expected to require new, unique, and unplanned support, or will place additional burdens on the existing and projected intelligence architecture.

2.5.2. Leverage related information contained in acquisition documents such as the ISP, Life-Cycle Mission Data Plan (LMDP), or Program Protection Plan (PPP). Acquisition documents listed in Reference [5] Enclosure 1 Table 2 can greatly assist with information on intelligence support, such as IMD availability, Counterintelligence (CI) Support Plans (CISPs), etc.

2.5.3. Review DoDAF products for intelligence requirements based on information and data flow plans that may impact the intelligence support categories such as Intelligence Planning and Operations Support and Intelligence Interoperability. For all identified intelligence requirements, address what intelligence infrastructure (e.g., platforms, systems, software, facilities, etc.) and resources will be required to collect, compile, store, analyze, and disseminate the required intelligence. Include a StdV-1 (Standards Profile) when standards apply to solution elements (this is particularly relevant to GEOINT, imagery, FMV, etc.). For further information on intelligence interoperability including definition, details and criteria required for intelligence requirements certification, reference paragraph 2.6.4 on page B-G-G-13.

2.5.4. Account for the resources required to augment intelligence support, in cases where requirements exceed the IC's ability to support, in the Program Affordability section of the capability requirements document.

2.5.5. Trace requirements to impacted performance attributes (KPPs, KSAs, and APAs) where applicable, and articulate potential coordination between materiel and non-materiel solutions.

2.5.6. Address intelligence interoperability requirements at both the system level (the ability of the system to produce data and metadata standards-compliant information, and exchange data and products with similarly compatible systems) and the operational level (within which the capability solution will function with operations, and C2 systems and processes).

2.5.7. Identify all security requirements or considerations needed to support the capability solution, and address how those security considerations will be satisfied whenever included in respective support category requirements. Ensure classification levels, information sharing or releasability, certifications, and facility implications for receiving, using, and storing data are addressed. If the capability solution will require or transmit Top Secret/Sensitive Compartmented Information, address appropriate physical security concerns (accreditation and use of a Sensitive Compartmented Information Facility) where required. For capability solutions using IS that have intelligence authorities as designated accrediting authorities, ensure interoperability test plans include security-testing considerations.

2.5.8. Intelligence Supportability. Introduce the paragraph with a general description of the types and level of required intelligence support to enable the program's intended capability, consistent with other document sections and considerations in the CDD paragraph, above.

2.5.8.1. Intelligence Support Category Requirements. Identify and address support requirements, potential shortfalls, and efforts to satisfy shortfalls, or state there are no requirements, for all the intelligence supportability categories below. (For category descriptions, see Section 2.6.). Be as specific as possible and include as many qualitative and quantitative attributes as possible.

2.5.8.1.1. Intelligence Manpower Support

2.5.8.1.2. Intelligence Funding Support

2.5.8.1.3. Intelligence Planning and Operations Support

2.5.8.1.4. Intelligence Interoperability

2.5.8.1.5. Targeting Support

2.5.8.1.6. Intelligence Mission Data Support

2.5.8.1.7. Space Intelligence Support

2.5.8.1.8. Counterintelligence Support

2.5.8.1.9. Intelligence Training Support

2.5.8.2. If requirements are discussed in other places within the document or in other documents (such as CI Support requirements addressed in a capability solution's PPP), provide cross-references to those paragraphs or documents.

2.6. Intelligence Support Category Descriptions. General descriptions of intelligence support requirement categories follow to assist Sponsors in identifying areas where a capability solution will likely need support.

2.6.1. Intelligence Manpower Support.

2.6.1.1. This category is to be addressed if the capability solution will require intelligence personnel for development, testing, training, and/or operations. Depending on the maturity of the capability solution, a Manpower Estimation Report (MER) may have been completed. If a MER shows that intelligence manpower changes will be required to support the fielding of the capability solution, a summary of intelligence implications from that report is to be included in this support category.

2.6.1.2. Address whether existing skills and specialties suffice, or if specific skills are required for support. Address how existing intelligence manpower resources will meet the capability solution's intelligence support requirements or whether the capability solution will require additional, dedicated intelligence personnel from within the sponsor's organization, by leveraging support from other organizations, or by training new personnel to fill the anticipated support requirements.

2.6.2. Intelligence Funding Support.

2.6.2.1. This requirement category is to be addressed if the capability solution or supporting efforts will require, or depend upon, intelligence funding. Special attention must be given to the requirement of IMD early in the capability lifecycle, including the assessment of IMD-dependent alternatives during AoAs and consideration of resourcing for IMD production prior to Milestone A.

2.6.2.2. Address whether, and to what extent, the capability solution relies upon intelligence capabilities that have not yet been provided dedicated funding, or have not received necessary approvals to begin operations or remain operational.

2.6.3. Intelligence Planning and Operations Support.

2.6.3.1. This category includes support requirements derived from the six interrelated categories of intelligence operations included in the Joint Intelligence Process (planning and direction; collection; processing and exploitation; analysis and production; dissemination and integration; and evaluation and feedback). It also includes support requirements from the different intelligence disciplines (signals intelligence (SIGINT), geospatial intelligence (GEOINT), etc.). Sponsors address interoperability requirements with Service, national and coalition elements in each Joint Intelligence Process step and intelligence discipline, where applicable.

2.6.3.2. Planning and Direction.

2.6.3.2.1. This category includes the receipt, identification, and prioritization of intelligence requirements; the development of concepts of intelligence operations and architectures; tasking appropriate intelligence elements for the collection of information or the production of finished intelligence; and, submitting requests for collection, exploitation, or all-source production support to external, supporting intelligence entities.

2.6.3.2.2. Sponsors must address whether mission-planning requirements have been considered and identified, including manpower, systems, tools, mission-planning data (Red, Gray, Blue, and White) or other non-materiel requirements at intelligence units, personnel training on systems architecture, and compatibility with current and future Defense Intelligence Information Environment (DI2E) architecture.

2.6.3.3. Collection.

2.6.3.3.1. Collection includes activities related to the acquisition of required data in order to satisfy specified requirements. This is managed by collection managers, whose duties include selecting the most appropriate, available asset(s) and associated Processing, Exploitation, and Dissemination (PED), and then tasking selected asset(s) and associated PED to conduct collection missions.

2.6.3.3.2. Collection management support refers to the required personnel, expertise, training, and systems needed to ensure intelligence information requests are submitted through the appropriate channels; that intelligence collection assets (e.g., Service, national, joint, coalition, multinational) are effectively employed to collect the required information; and that the collected information is disseminated to the entity that made the original request and to all other end users requiring such information.

2.6.3.3.3. Address requirements for appropriate collection management resources, tools and infrastructure, and level of national/coalition interoperability to support the capability solution. Address types of intelligence information needed (form and substance), collection asset(s) or collection asset capabilities that will be needed to collect the requested information, and compliance with data and metadata standards.

2.6.3.3.4. Collection also includes support that the capability solution will require from the different intelligence disciplines:

2.6.3.3.4.1. SIGINT, including communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT). SIGINT support should include any requirements for intelligence produced by exploiting foreign communications systems and non-communications emitters.

2.6.3.3.4.2. Human Intelligence (HUMINT). The category of intelligence derived from information collected and provided by human sources.

2.6.3.3.4.3. Measurement and Signature Intelligence (MASINT). MASINT is information produced by quantitative and qualitative analysis of physical attributes of targets and events to characterize, locate, and identify them. MASINT techniques are used to support signature development and analysis, to perform technical analysis, and to detect, characterize, locate, and identify targets and events. MASINT is derived from specialized measurements of physical phenomena intrinsic to an object or event, and it includes the use of quantitative signatures to interpret the data. The measurement aspect of MASINT refers to actual measurements of parameters of an event or object such as the demonstrated flight profile and range of a cruise missile. Signatures are typically the products of multiple measurements collected over time and under varying circumstances. These signatures are used to develop target classification profiles, discrimination, and reporting algorithms for operational surveillance and weapon systems.

2.6.3.3.4.4. GEOINT. GEOINT, in relation to Intelligence Operations and Planning, is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical and geophysical features and geographically referenced activities on the earth. GEOINT, in this regard, consists of imagery, imagery intelligence, and geospatial information. Geospatial information includes topographic maps, safety of navigation aeronautical and SoN nautical charts, geodetic data, and related products (e.g., world magnetic model and gravity model). The DoD Functional Manager responsible for the production and dissemination of GEOINT is the National Geospatial-Intelligence Agency (NGA). NGA is responsible for the production, maintenance, and distribution of the World Geodetic System 1984 (WGS 84) to support DoD navigation systems. To fulfill geospatial requirements for their capability solutions, Sponsors must comply with the processes and milestones identified in References [93], [94], and [95] to accommodate the planning, allocation, and de-confliction of geospatial information and services (GI&S)-related collection, analytic, and dissemination resources that are consistently in high demand. Programs that send, produce and/or receive GEOINT data and/or services will conform to mandated GEOINT standards cited in the DISR. Refer to Intelligence Interoperability for more details. Systems that require unique GEOINT products and services must identify those requirements within capability requirements documents to ensure the products and services transition into the acquisition process. New or upgraded systems that require an increase in coverage or production capacity from the NGA baseline must also forecast the requirements within the JCIDS process. Because of the potential resource demands of these support requirements and their resulting effect on the GEOINT community, requirements must be qualitatively and quantitatively identified at the earliest possible point in the JCIDS process and updated IAW References [93] and [154]. Details include the required data, coverage, scale, timelines, formats, numeric quantity of products, accuracy, resolution level (e.g., imagery and/or Digital Terrain Elevation Data (DTED) levels) and necessary update requirements (periodic versus as-needed).

2.6.3.4. Processing and Exploitation.

2.6.3.4.1. Data initially received from the sensor, commercial providers, foreign partners and other US Government agencies, arrives in various forms depending on the nature of the sensing device. Depending on the source, the raw input may be in the form of digitized data, unintelligible voice transmissions, or large digital files containing multi-beam bathymetric data to un-rectified images of the Earth. This collection output is converted by sensor-specific processing measures into visual, auditory, or textual information, which then can be used by foundation and intelligence analysts and other consumers. The data conversion may be automated using algorithmic fusion, cuing, data analytics and automated exploitation. Exploitation entails the further translation and contextualizing of information into a product that the planner, decision maker, or intelligence analyst can cognitively assimilate. Exploitation efforts will vary greatly by the required specific products; examples should include format specifications, accuracy requirements, production timeline needs, and refresh rates requirements.

2.6.3.4.2. Address whether sufficient personnel and resources will be in place for effective processing and exploitation. Where possible, address required data, coverage, scale, timeliness, formats, accuracy, resolution level (e.g., imagery and/or DTED levels). Consider whether the intelligence architecture will support the volume of data requiring processing. Ensure data is in standard formats to support interoperability. Dependent upon the requirements of Sponsor's capability solution being supported, consider what types of delivery/communications systems will be required and the volume of information that will be delivered. In addition, see the section on targeting support, for exploitation requirements supporting targeting and coordinate-seeking weapons.

2.6.3.5. Analysis and Production.

2.6.3.5.1. During analysis and production, intelligence is produced from the information gathered by collection capabilities, and from the refinement and compilation of intelligence received from external organizations. All available processed information is integrated, evaluated, analyzed, and interpreted to create products that will satisfy users or requesters. Intelligence products can be presented in many forms; they may be oral presentations, hard copy publications, or electronic media accomplished by units and organizations at every echelon and including reach back locations. Whereas collection, processing, and exploitation are primarily performed by specialists from one of the major intelligence disciplines, analysis and production is done primarily by all-source imagery and foundation analysts that fuse together information from all intelligence disciplines.

2.6.3.5.2. Address the necessary or desired product format (electronic versus paper), production timeline, and necessary update requirements (periodic versus as-needed) that will be available and have been requested to support

their capability solutions. Consider whether sufficient personnel and resources will be in place for effective analysis and production.

2.6.3.6. Dissemination and Integration.

2.6.3.6.1. The timely distribution of critical information, Foundation GEOINT, and finished intelligence to appropriate consumers, readily accessible by the user. The movement toward a communications and computers centered environment has reduced the technical challenges related to information dissemination. Nevertheless, intelligence infrastructure (such as intelligence networks, systems, and software) and intelligence resources (such as funded programs or manpower) remain critical components of information delivery. Another measure of dissemination support is compliance with IC and DoD data and IAW metadata standards. Personal, networked, and database data transfers are all means of dissemination. The diversity of dissemination paths reinforces the need for communications and computer systems interoperability among joint and multinational forces, component commands, DoD organizations, and the interagency community.

2.6.3.6.2. Address the requirements of the capability solution being supported, which may include: timeliness and means of delivery, interoperability of delivery/communications systems (including requirements for interoperability with coalition and other organizations' systems), format of information delivered (including compliance with data and metadata standards), and information/product storage location, capacity and accessibility.

2.6.3.7. Evaluation and Feedback.

2.6.3.7.1. Evaluation and feedback occur continuously throughout the intelligence process, and as an assessment of the intelligence process as a whole. Intelligence personnel at all levels, as well as users of intelligence, should assess the execution of the intelligence tasks being performed to identify deficiencies within the intelligence process and determine if intelligence requirements are being satisfied. The goal of evaluation and feedback is to identify issues as early as possible to minimize information gaps and to mitigate capability shortfalls.

2.6.3.8. When possible, address capability solution requirements for means, formats, information needs and periodicity of assessments to support decisions about reprioritization of intelligence requirements, shifts in collection emphasis, changes to analytic levels of effort, reallocation of available intelligence assets, training of intelligence personnel, and the development of new intelligence capabilities.

2.6.4. Intelligence Interoperability.

2.6.4.1. The term intelligence interoperability is derived from the existing definitions of intelligence and interoperability currently found in References [10] and [96] respectively.

2.6.4.2. Intelligence interoperability is defined as the ability to receive, produce, store, and/or share intelligence data, products, services, and/or processes with similarly compatible systems; and, to render that data, product, service, and/or process to other applicable systems in a readily available format. Intelligence interoperability includes both the technical exchange of information (data) and the operational effectiveness of that exchanged information (service and processes). Intelligence interoperability is more than just information exchange; it includes harmonization of intelligence systems, processes, procedures, organizations, and missions.

2.6.4.3. The intent of intelligence interoperability guidance in capability requirements documents is to account for when, where, and how a capability interacts (e.g., receiving, producing, and/or sending information) with other intelligence capabilities of the IC, Services, and Coalition partners. The intelligence interoperability paragraph must be consistent with the Operational Context, Capability Discussion, Performance Attributes, DOTmLPF-P, and Joint Interoperability sections of the capability requirements document.

2.6.4.4. The Sponsor must address the requirements of the capability solution being supported, including interoperability of delivery/communications systems (including requirements for interoperability with Service, Coalition, and other organizations' systems), format of information delivered (including compliance with data and metadata standards), and information/product storage location, capacity and accessibility. The Sponsor must also ensure:

2.6.4.4.1. The intelligence dissemination infrastructure is available, suitable, and sufficient throughout the program's expected lifecycle. Specifically, that the program has an information exchange path with the IC and is capable of sending and/or receiving information and data to/from other systems. The Sponsor shall document assurance, or requirement, that the volume of data sent and/or received is within IC bandwidth limitations.

2.6.4.4.2. The interoperability interfaces, and/or information exchange requirements are accurately identified in applicable DoDAF architecture products. Include a StdV-1 (Standards Profile) when standards apply to solution elements (this is particularly relevant to GEOINT, imagery, FMV, etc.) Address intelligence interoperability requirements at both the system level (the ability of the system to produce data and metadata standards-compliant information, and exchange data and products with similarly compatible systems) and the operational level (within which the capability solution will function with operations, and C2 systems and processes).

2.6.4.4.3. The program shall document strategies to achieve conformance with applicable data and metadata standards, including -mandated DoD Information Technology Standards Registry (DISR) technical standards, Standardization Agreements (STANAGs), Allied Engineering Documents (AED), etc. Sponsor must coordinate with the IC and/or applicable Functional Manager (e.g., NGA for GEOINT and IAW References [97]and [98]) to ensure the

capability can send, produce, and/or receive conformant data and services. In addition, the Sponsor must submit a waiver IAW Reference [99] to implement a standard other than a mandated and/or emerging DISR standard.

2.6.4.4.4. The program documents the requirement to be accredited to receive and protect IC data. If the system or capability uses TS/SCI traffic, the Sponsor shall ensure compliance with Director, Central Intelligence (DCI) security directives and IC ITE standards such as cited in References [100] and [101].

2.6.4.4.5. For capability solutions using IS that have intelligence authorities as designated accreditation authorities, ensure interoperability test plans include security-testing considerations.

2.6.5. Targeting Support.

2.6.5.1. Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering commander's guidance and objectives, planning requirements at all warfare levels, and operational requirements and capabilities. See Reference [102].

2.6.5.2. Targeting support refers to the intelligence information, infrastructure, or required resources:

2.6.5.2.1. For target development, including derivation of coordinates and target materials production, validation, nomination, and prioritization.

2.6.5.2.2. To support capabilities analysis and force assignment.

2.6.5.2.3. To support mission planning, including support such as weaponeering, target imagery notation, collateral damage estimation, and coordinate verification.

2.6.5.2.4. To support operational execution, including time-sensitive targeting support such as target identification, coordinate derivation, and weaponeering.

2.6.5.2.5. To support the combat assessment process, including battle damage assessment (BDA), munitions effects assessment (MEA), and supporting re-attack recommendations.

2.6.5.3. Sponsors must consider intelligence support to targeting if their capability solution will employ, or will rely upon the employment of, offensive kinetic and non-kinetic capabilities. Intelligence targeting support shortfalls may negatively impact the capability solution's successful development, on-time delivery schedule, and ultimately its operational status (i.e., intelligence support to targeting is a broad category that encompasses munitions and all associated capability solutions relying upon the munition).

2.6.5.4. Intelligence support to targeting may also be required during munition and other non-kinetic offensive capability design, development, and testing to help ensure the anticipated performance. (MEA and BDA studies may help identify gaps in FA capabilities.) Sponsors with capability solutions that will

employ or rely on the employment of munitions must also consider intelligence support to targeting, and identify and address intelligence support requirements and shortfalls, if any, regarding not only their capability solution, but also the munitions it will employ or rely upon.

2.6.5.5. Examples of targeting products include target lists, target folders, target materials, modeling and simulation products, and collection and exploitation requirements to support targeting and target briefs. Examples of targeting services include weaponeering, casualty and collateral damage estimation, point positioning/coordinate mensuration, and verification and tactical mission planning support.

2.6.5.6. Targeting support may overlap with the GEOINT support category because many targeting services rely upon and/or incorporate geospatial products or information. Coordinate-seeking weapons, or weapons that can or will be able to operate in a coordinate-seeking mode, must declare required target location error -- expressed as circular and linear error in meters or feet -- with an associated confidence level reported at 90 percent.

2.6.5.7. Address requirements for support to target development, mission planning, precise positioning, BDA, MEA, weaponeering, the anticipated volume of targets to be managed and numbers of target folders to be produced and associated targets or aim points to plan for during mission planning. Also, address capability targeting certification and accreditation requirements IAW Reference [103].

2.6.6. Intelligence Mission Data (IMD) Support.

2.6.6.1. IMD is DoD intelligence used for programming platform mission systems including, but not limited to, the functional areas of: Signatures, Electronic Warfare Integrated Reprogramming (EWIR), Order of Battle (OOB), Characteristics & Performance (C&P), and GEOINT. See References [45] and [104].

2.6.6.1.1. Signatures. The distinctive characteristics or set of characteristics that consistently recur and identify a piece of equipment, materiel, activity, or event. Signature support is the provision of such data to capability solutions that use signatures in their design, development, testing, training, or operations of sensors, models, or algorithms for the purpose of: combat identification; blue force tracking; targeting; detecting or identifying activities, events, persons, materiel, or equipment. This data may be used by intelligence analysts, automated systems, and system design and development engineers to analyze and identify threats or the patterns of use for an adversary system.

2.6.6.1.2. EWIR. Assessed, all-source intelligence data on adversary and non-adversary commercial systems, including technical parametric and performance data, observed electronic intelligence data on foreign emitters from the National Security Agency (NSA), and engineering-value/measured data on domestic emitters.

2.6.6.1.3. OOB. The identification, command structure, strength, and disposition of personnel, equipment, and units of an armed force participating in field operations. OOB supporting mission data file (MDF) generation emphasizes “fact of presence” or “fact of possession” for equipment in known area of operations. (Traditional OOB describes force structure and size in “garrison.” Equipment deployed to another theater or country is frequently not tracked. Fact of presence or possession accounts for equipment routinely operating in, but is not assigned to, an area of operations.)

2.6.6.1.4. C&P. All-source derived assessments of foreign military system capabilities and physical attributes.

2.6.6.1.5. GEOINT. GEOINT IMD provides programs with mapping, charting and geodesy, geospatial information, and other GEOINT data, products and services to support operations, navigation (including Safety of Navigation), terrain visualization, targeting, and characterization of the physical and man-made environments. It is important that GEOINT IMD requirements be addressed early in the development of a capability requirement and documented for the entire system lifecycle.

2.6.6.1.5.1. GEOINT provides two irreplaceable components that contribute to the effectiveness of weapons and weapon systems: a framework (WGS 84) that renders other intelligence actionable by virtue and referencing it to a four dimensional space-time context and critical qualitative and quantitative information to describe the physical and functional characteristics of the political, economic, military, social, informational, and infrastructure components of an adversary’s capabilities. The fusion of intelligence (including imagery-based MASINT) with geospatial information to create GEOINT conveys understanding of enemy assets and actions that play a dominant role in determining weapon and weapon system effectiveness. Early and concise identification of GEOINT shortfalls for planning and execution to optimize weapon and weapon system effectiveness is a matter of critical concern when NGA must justify requirements for resources and apportionment of those resources within the agency. An example of such GEOINT shortfalls would be the identification of routine data exploitation and production requirements for the construction details of buildings that affect the performance of miniaturized munitions. Another example would be concise description of man-made features and demographic distributions in urban areas where planned operations must consider high-fidelity estimation of collateral damage risks.

2.6.6.2. IMD requirements must be considered as early as the AoA when one or more of the alternatives under consideration are likely to be dependent upon IMD to ensure mission effectiveness. Consideration is to be given for alternatives that are not IMD-dependent or those that can be satisfied by IMD already produced by the IC. Alternatives requiring additional IMD production by the IC should only be considered where the value of the additional mission effectiveness exceeds the cost associated with generating and maintaining the additional IMD.

2.6.6.3. CDDs are to state whether the capability solution requires IMD. If the capability solution is IMD dependent, include a list of the relevant IMD functional area(s), an assessment of the IC's ability to support those requirements, and a reference to the capability solution's LMDP.

2.6.6.4. In cases where different levels of IMD contribute to different levels of performance, Sponsors should use a systems engineering operational assessment methodology to evaluate requirements, and assess the criticality of different IMD levels and potential shortfalls, against performance attributes. Sponsors should also address IMD criticality, per the risk levels described in table below, during FCB capability reviews. Specifically, Sponsors should describe the impact on the capability when IMD shortfalls exist. In such circumstances, the Sponsor should be prepared to describe mitigating strategies including change in CONOPS, change in design, or a recommendation to offset shortfalls through increased resourcing when a decrement in the capability delivered is unacceptable.

APPROVAL AUTHORITY MDA=I PEO=II PM=III **RESULTANT IMD**		**RESULTANT SHORTFALL RISK**			
		Available	**Partially Available**	**Potentially Available**	**Unobtainable**
1	**Unacceptable:** Requirement that if not satisfied results in an unacceptable operational mission/ program(s) impact (operational workaround is not possible).	**III**	**I**	**I**	**I**
2	**Significant:** Requirement that if not satisfied results in significant operational mission/program(s) impact (operational workaround is available and must be applied).	**III**	**I**	**I**	**I**
3	**Partial:** Requirement that if not satisfied results in degradation that is acceptable to the operational mission/program(s) (operational workaround is optional) (includes broadly specified requirements).	**III**	**II**	**I**	**I**
4	**Limited or No:** Requirement that optimizes functionality; however, if not satisfied, has minimal degradation to the operational mission/program(s) (includes beyond FYDP requirements forecasts to support strategic planning)	**III**	**III**	**III**	**II**

Definitions:
- **Available:** Data is available for this system for all requested system parameters.
- **Partially Available:** Data is available for this system for some, but not all requested parameters; or data is available, but not within the requested specification.
- **Potentially Available:** The Defense Intelligence All-Source Analysis Enterprise (DIAAE) does not have the requested data for this system, but can provide it given additional resources, manpower, collection capability, or reprioritization of production planning.
- **Unobtainable:** The DIAAE cannot provide this information due to scientific, technical, or legal limitations, or due to political sensitivities.

Figure B- 26: IMD Risk Table

2.6.6.5. IMD production and collection requirements that can be met by an acquisition program and are validated by the capability requirements community are included in the capability solution's LMDP IAW Reference [45]. IMD production and collection requirement thresholds that exceed the IC's ability to support, must be included in the program affordability section of CDDs as a cost associated with developing the capability solution.

2.6.6.6. Among IMD requirements, address whether all signature support (including coverage, timeliness, content, fidelity, security, and scalability), and denial and deception support was considered and addressed. In addition, address whether sufficient analytical support is available to provide EWIR and C&P data, and whether all categories of data can be collected (i.e., White, Red, Blue, or Gray).

2.6.6.7. DIA/TLA will evaluate the program's actionable IMD requirements derived from the LMDP, or for IMD dependency if an LMDP has not been submitted. If DIA/TLA determines that a program is IMD-dependent and an LMDP was not submitted, they will submit a comment and supporting rationale via CRM during JCIDS staffing for Sponsor adjudication. Such comment should be sufficient cause to initiate discussion between the Sponsor, Program Office, and the IC to develop an LMDP. For IMD-dependent programs, DIA/TLA will prepare an evaluation summarizing IMD availability and costs for gaps. The Sponsor should be prepared to discuss IMD supportability and address risk mitigation for IMD shortfalls with the Lead and BA FCBs during the JCIDS staffing. DIA/TLA IMD evaluation and recommendations will be included as a condition of intelligence certification.

2.6.7. Space Intelligence Support.

2.6.7.1. Space intelligence support refers to requirements for space-based capability solutions, other capability solutions relying upon space-derived capabilities, and platforms that perform space control or space support. Reference [105] provides additional descriptions relative to this topic. This category also includes intelligence information, infrastructure, or resources that provide space-specific intelligence analysis on foreign space capabilities.

2.6.7.2. The Sponsor should address the requirements of the capability solution being supported, which may include: timeliness and means of delivery, anticipated throughput, interoperability of communication systems (including requirements for interoperability with coalition and other

organizations' systems), format of information delivered (including compliance with data and metadata standards), and information/product storage location, capacity and accessibility.

2.6.7.2.1. The Sponsor should provide an assessment, if possible, of the existing space-based infrastructure capacity to support the needs of the capability in development, or if the infrastructure may require augmentation. If the capability in development will rely upon future or planned space-based capabilities, or if the existing space-based capability requires augmentation, the Sponsor should consider impacts to the capability in development and provide mitigating strategies if the existing or planned space-based capability is insufficient.

2.6.7.2.2. Sponsors should describe the types of interactions depicted in applicable DoDAF products including the capability's need to send and/or receive information through or from space-based platforms, types of products, and anticipated throughput volume, capacity, and frequency.

2.6.7.2.3. Identify all security requirements or considerations needed to support the capability solution and address how those security considerations will be satisfied. Ensure classification levels, information sharing or releasability, certifications, and facility implications for receiving, using, and storing data are addressed and in compliance with References [100] and [101]. If the capability solution will require or transmit TS/SCI information, address appropriate physical security concerns (accreditation and use of SCIF) where required.

2.6.8. CI Support.

2.6.8.1. Pursuant to Reference [106], CI support encompasses the process of gathering information on, and activities conducted to counter, adversary or other collection activities directed against U.S./allied forces, other intelligence activities, sabotage or terrorism conducted by, or on behalf of, foreign governments, foreign organizations, foreign persons or international terrorist entities. CI support includes the intelligence information, infrastructure, or resources used to educate acquisition communities on those threats. CI Support also helps acquisition communities establish plans, tools, or techniques to protect designated S&T information.

2.6.8.2. CI support may include a number of activities applied throughout a capability solution's lifecycle, from providing threat awareness education to scientists and engineers performing fundamental research, to the implementation of a PPP. At a minimum, the following actions are required in order to fully identify CI Support requirements and devise adequate capability protection measures. Overarching guidance and direction can be found in Reference [107].

2.6.8.2.1. Identification of Critical Program Information (CPI). CPI is U.S. capability elements that contribute to warfighters technical advantage, which, if compromised, undermines U.S. military preeminence. U.S. capability

elements may include, but are not limited to, software algorithms and hardware residing on the system, its training equipment, or maintenance support equipment. Programs shall identify CPI per References [108] and [109].

2.6.8.2.2. Technology Targeting Risk Assessments (TTRAs) help DoD Components identify threats to CPI. Completion of a TTRA detailing the threat to the technology, must be completed.

2.6.8.2.3. Upon completion, the TTRA is forwarded to the Service CI organization (Military Department CI Organization or MDCO) to incorporate into the CI threat assessment describing foreign intelligence threat to the program.

2.6.8.3. Informed by the TTRA and CI threat assessment, the Sponsor must address the required CI Support activities needed to provide adequate program security and protection throughout the capability's lifecycle. The Sponsor must also identify the organization(s) conducting the activities, provide information on the TTRA and CI threat assessments, and provide the CISP. The Sponsor should identify potential shortfalls if CI support requirements are not resourced, and provide mitigating strategies to ensure program security. In addition, the Sponsor should select from among the following activities including in the CI Support requirements paragraph, as applicable.

2.6.8.3.1. Providing foreign collection threat information to assist personnel supporting research, development, and acquisition (RDA) programs in identifying CPI and developing threat-based

2.6.8.3.2. Participating in installation-level, program-level, or facility-level threat working groups to inform participants of foreign collections threats to RDA activities.

2.6.8.3.3. Coordinating with security managers, intelligence, and information assurance personnel to aid in threat identification and the establishment of countermeasures designed to detect and mitigate foreign and international terrorist cyber-associated threats to RDA programs and activities.

2.6.8.3.4. Reviewing RDA-affiliated documents, PPPs, and Intelligence Information Reports to assist in developing threat awareness training and requesting analytical support.

2.6.8.3.5. Evaluating individual and organizational awareness of foreign collection threats to determine vulnerabilities of FIE collection, assessing the effectiveness of existing countermeasures, and assisting RDA security personnel develop new countermeasures.

2.6.8.3.6. Providing foreign collection threat assessments, advisories, or related IC analytical products to supported RDT&E facilities, RDA programs with CPI, cleared defense contractors (CDCs), and for use in constructing threat awareness training.

2.6.8.4. This process serves to inform the development of the Counterintelligence Support Plan (CISP), a supporting appendix to the PPP.

2.6.9. Intelligence Training Support.

2.6.9.1. Some capability solutions may require intelligence personnel to provide specialized training to support part or all of a given capability solution's lifecycle.

2.6.9.2. The training requirement may include training additional personnel in existing training programs and/or in a new, unique training program that will be developed to support the capability solution. In either case, the requirement for training to support part or all of a capability solution's lifecycle must be identified, analyzed, and declared as soon as possible to permit sufficient lead-time to facilitate curriculum development and cultivate personnel with the required skills needed to support sponsor's capability solution.

2.6.9.3. Intelligence Training Support may require the production of new training documents or product lines facilitating training in on-line or in-residence venues.

2.6.9.4. Sponsors must address the anticipated required manpower to support the capability solution, expected required certifications, skill specialties (e.g., Air Force Specialty Code, Military Occupational Specialty), schools/courses, and language skills. Sponsor must also address whether there will be a requirement for a new or unique training program (with appropriate curriculum and product support) needed to support the Sponsor's capability solution.

3. Intelligence Supportability Review and Assessment.

3.1. The intelligence supportability review analyzes a capability's intelligence support requirements for completeness and supportability, and evaluates what is required from, or contributes to, the IC throughout a capability solution's lifecycle. Extensive coordination, collaboration, and analysis are critical to ensure the full range of potential intelligence supportability issues are addressed.

3.2. Associated Intelligence Support Requirements. Sponsors are responsible for identifying all associated intelligence support requirements and shortfalls related to their capabilities, to enable a complete analysis of the program in support of the intelligence certification.

3.2.1. Completeness refers to whether a Sponsor's document adequately addresses the applicable intelligence supportability requirements related to the proposed capability requirements. Completeness also requires Sponsors address how their capabilities comply with security considerations, and classification of information and systems; procedures or authority to release or handle classified information, including intelligence data; interoperability with operations, C2, and supporting intelligence systems; and, how the capability may impact intelligence strategy, policy, and architecture planning.

3.2.2. Supportability refers to the availability, suitability, and sufficiency of required intelligence support needed by a capability. Assessing supportability requires a comparison of the Sponsor's stated operational/capability requirements with the expected intelligence support capabilities, throughout a capability solution's projected lifecycle. The ability to adequately assess supportability depends upon the completeness of the Sponsor's declaration of the capability's intelligence support requirements and must be evaluated within the context of any shortfall mitigation strategies identified. Availability refers to whether the intelligence data, information, infrastructure, or resources are, or are expected to be, available throughout the capability solution's projected lifecycle; suitability refers to whether the required intelligence data, information, infrastructure, or resources are, or are expected to be, appropriate to support the capability; and, sufficiency refers to whether the intelligence data, information, infrastructure, or resources are, or are expected to be, adequate to support the Sponsor's capability.

3.3. Intelligence Supportability Assessment Process.

3.3.1. Intelligence supportability assessments and certifications are conducted during the normal staffing of capability requirements documents as described in Enclosure A of this manual.

3.3.2. Document Review and Commenting Stage. During this stage, the threat assessment, including CIPs and the intelligence supportability content of the capability requirements document are reviewed. Any recommended changes to the threat environment information and References, development of new and/or updating of approved CIPs associated with threat-dependent capability requirements, and changes to requirements associated with intelligence supportability categories, which impact the ability to issue the intelligence certification, are documented and submitted for Sponsor adjudication.

3.3.2.1. DIA assesses the Sponsor's threat information, threat analysis, and CIPs by evaluating the Sponsor's capability requirements documents for appropriateness of judgments concerning the extent and scope of threats, ensuring consistency with DIA-or Service-approved threat products, and ensures that the Sponsor has included current threat products, information, and findings.

3.3.2.2. DIA (or Service-level threat validation authority, as appropriate) will also evaluate the capability performance attributes that are potentially threat-sensitive or dependent. If DIA determines that a CIP is warranted, procedures described in this annex will be followed.

3.3.2.3. The Intelligence Mission Data Center (IMDC) and other commenters will submit recommended changes on IMD support requirements in CDDs, and link IMD to capability performance attributes, as needed. The IMDC will focus on whether the complete set of IMD requirements were articulated in the CDD and program LMDP.

3.3.2.4. J-283/IRCO assesses the completeness and supportability (availability, suitability, and sufficiency) of the requirements identified for each intelligence support category, and whether the Sponsor considered all content guidance included in Paragraph 2 of this annex.

3.3.2.4.1. When reviewing ICDs, which do not include the Intelligence Supportability paragraph, J-283/IRCO assesses whether the program contains potential intelligence support requirements by determining if the capability will require data and/or information from the IC, or will produce data and/or information that will flow to the IC, to support research, design, development, test and evaluation, and operations. If either condition is present, the capability will be designated Intelligence-sensitive, and must include content described in Paragraph 2.6.3 of this annex.

3.3.2.4.1.1. If the capability is Intelligence-sensitive, it should then undergo a more thorough Intelligence Supportability Assessment (ISA) as part of the capability's AoA. The goal of the ISA is to effectively identify derived intelligence support requirements and deficiencies, along with associated impacts to both acquisition and operational capability if the required intelligence support is not provided. Sponsors/PMs and the IC can then develop plans and strategies to support these derived intelligence requirements, and ensure the requisite supporting intelligence infrastructure needed to successfully acquire and employ future joint capabilities is available. The results of the ISA should be included in the AoA Report to inform the JCIDS Post-AoA review and the Milestone A acquisition decision, and provided prior to Milestone B and Milestone C decisions for capability solutions.

3.3.3. Comment Adjudication Stage. During this stage, Sponsors adjudicate each comment submitted to the satisfaction of the reviewer. However, adjudication of any comments related to intelligence certification must be completed to the satisfaction of J-283/IRCO, unless the capability requirements document, and the supporting certifications and endorsements, are delegated to an independent validation authority IAW Enclosure A of this manual. Active coordination between the Sponsor, reviewer, and J-283/IRCO is expected to facilitate comment adjudication.

3.3.4. FCB Draft Review Stage. During this stage, J-283/IRCO shall review the final adjudicated CRM and updated capability requirements document to ensure that all comments concerning intelligence have been satisfactorily adjudicated and incorporated.

3.3.4.1. J-283/IRCO will request DIA/TLA make a determination on approval or non-approval of the threat, including CIPs, for that portion of the intelligence certification.

3.3.4.2. J-283/IRCO will coordinate with, and assist, the Sponsor and assigned FCB in the assessment of IMD support requirements and shortfalls, and determination of sufficient levels of IMD to satisfy operational requirements, during FCB capability reviews, in which the FCBs should:

3.3.4.2.1. Assess identified supporting tasks and criticality levels of IMD needs.

3.3.4.2.2. Assess the mapping of IMD requirements to supporting tasks.

3.3.4.2.3. Assess and approve IMD criticality levels, types of IMD needed, and IMD availability and need dates.

3.3.4.2.4. Assess and approve IMD sufficiency and risk management actions proposed for any identified IMD shortfalls.

3.3.4.2.5. Provide a prioritized list of IMD requirements for any identified shortfalls to the BA FCB, which will advocate IMD priorities and production requirements to the IC.

4. Intelligence Certification.

4.1. The intelligence certification is a statement of adequacy and assesses whether the IC can provide the required support to the acquisition and operational communities. The certification is the result of collaboration and analysis that leverages the expertise and unique perspectives of all applicable offices within DIA, NGA, NRO, NSA, CCMDs, Service Intelligence organizations, and the Joint Staff J-2.

4.2. Collaborative Intelligence Certification Process. J-283/IRCO shall lead this collaborative intelligence certification process for the Joint Staff on behalf of the J-2 directorate. J-283/IRCO review and intelligence certification is conducted as part of validation of each capability requirements document, in support of each acquisition decision point, i.e., the ICD for Milestone A, the CDD for the Development RFP release decision point before Milestone B, and if required an updated CDD for Milestone C. In addition, J-283/IRCO review and intelligence certification is conducted as part of validation of Joint DCRs that have intelligence supportability impacts or affect capability solutions that received threat assessment and intelligence certification.

4.3. Intelligence Certification Procedures.

4.3.1. Once DIA/TLA approves the threat, and comments submitted during Document Review are adequately addressed and adjudicated to the satisfaction of the commenter and J-283/IRCO and associated changes made to the capability document, J-283/IRCO drafts the appropriate certification memorandum for signature.

4.3.2. For intelligence certifications that approve CIPs associated with threat-dependent capability requirements identified in an ICD, or for solution-specific threat dependencies associated with performance attributes identified in the CDD, the certification is valid until the next acquisition milestone, with a new intelligence certification to be generated during the validation of the successor capability requirements document.

4.3.3. In the event that the Sponsor initiates a change to the subject document, and the most recent threat assessment falls beyond the year of the

last threat assessment period, the Sponsor must request an updated threat assessment be conducted by DIA or the Service.

4.3.4. Upon first notification of either a CIP breach or threat change which impacts one or more of the program's approved CIPs, or a change to an intelligence program supporting or enabling the capability solution, via J-283/IRCO or other source, the Joint Staff Gatekeeper may recommend to the validation authority that a program's intelligence certification be reevaluated.

4.3.4.1. In cases of CIP changes or changes to intelligence supporting or enabling capabilities, staffing procedures similar to JCB/JROC Tripwire reviews will be used.

4.3.4.2. As multiple capability requirements and their associated capability solutions could be affected by the same CIP breach or changes to intelligence supporting or enabling capabilities, the FCBs and other stakeholders in the review process will consider impacts within and across the capability requirements portfolios.

4.3.4.3. Not every CIP breach or threat change will necessarily drive a change to capability requirements, or solution-specific performance attributes. The validation authority and other stakeholders must balance the potential increase to operational risk from not making a change to the capability requirements with the potential impacts to cost and schedule from making changes to capability requirements being addressed by an ongoing acquisition program.

4.3.5. J-283/IRCO tracks capabilities that have received certification without approved CIPs. J-283/IRCO recommends to the Joint Staff Gatekeeper that a capability is approaching a two-way review requirement and that its intelligence certification should be reevaluated. J-283/IRCO also engages the Service Intelligence staffs (A2, DIRINT, G2, and N2/N6) for insight into CIPs generated during this period for capabilities approaching a 2-year review requirement.

4.3.6. All programs introduced into staffing for limited review (e.g., KPP change), regardless of intelligence certification date, will be subject to full review for intelligence certification given the potential far-reaching impacts KPP and similar changes may have on associated CIPs and intelligence supportability, and to expose capability changes necessitated by changes in threat since the last certification.

4.3.7. In the event of a CIP breach relative to a program, J-283/IRCO will notify the Joint Staff Gatekeeper, also informing the Lead FCB, recommending that intelligence certification be reevaluated considering the outcome of the CIP breach risk mitigation processes.

4.3.8. DIA should work with each of the FCBs to define portfolios of threat topics in order to generate at least annual feedback on the status of CIPs aligned with the portfolio.

4.4. Intelligence certification shall affirm that:

4.4.1. The program or capability meets minimal requirements for intelligence support needs to completeness and supportability, and that an assessment concerning the program's impact on intelligence strategy, policy, and architecture has identified no significant shortfalls in current or planned intelligence support.

4.4.2. Any intelligence support or threat-related comments applicable to the program or capability have been appropriately adjudicated to the satisfaction of the entity submitting the comment and to J-283/IRCO, or otherwise resolved by the appropriate FCB WG, FCB, JCB, or JROC.

4.4.3. DIA/TLA has reviewed CIPs and threat information, including DIA- or Service-approved threat products used in the capability requirements document, and approves the threat section content pursuant to Reference [35].

4.4.4. DIA DO/OCI, when applicable, has validated the currency and relevancy of intelligence and CI analytical products used to assess the foreign collection threat and referenced in a PPP prior to major milestone decisions; conducted threat analysis of supply chain risk focusing on identifying foreign-affiliated capabilities that would enable an adversary to exploit vulnerabilities, maliciously modify a provided product or service, sabotage system function, or clandestinely extract data or information; and, verifies that applicable DIA- or Service-approved threat products are current.

4.4.5. For ICDs determined to be intelligence-sensitive, an ISA should be conducted against identified potential solutions during any AoA (or similar study) review; an ISA should begin as early as possible and continue throughout the entire acquisition lifecycle; and, its resulting findings should be used to evaluate intelligence support sufficiency.

4.4.6. Any projected shortcomings in joint intelligence support will be included in BA FCB analysis efforts as part of the CGA, to identify and prioritize capability gaps within the BA functional area.

4.5. Intelligence certification is effective only for the capability requirements document and its associated acquisition milestone. Intelligence certification memorandums will be posted in KM/DS and provided to the Joint Staff Gatekeeper for distribution to DJ-8, the Sponsor, and Lead and Supporting FCBs.

4.6. Intelligence certification serves as the enduring baseline for IMD requirements detailed in the LMDP for the lifecycle of the program. The intelligence certification granted for the CDD prior to Milestone B, or updated in the CDD prior to Milestone C, sets the baseline for IMD production requirements in post Milestone C operation of the system by the warfighter. In cases where additional IMD production is required, during development or during the O&S phase, intelligence supportability will be reviewed and re-certified to ensure appropriate tradeoffs are considered between IMD

requirements, system performance, and costs associated with additional IMD production.

4.7. Intelligence certification of documents protected by ACCM or SAP/SAR designation must also be reviewed and certified for intelligence supportability. Once notified by the Joint Staff Gatekeeper or J-8/SAPCOORD that a capability requirements document requires review, J-283/IRCO will coordinate with the Sponsor or J-8/SAPCOORD for appropriate access to conduct the review. While ACCM and SAP/SAR security restrictions preclude normal collaboration and coordination, J-283/IRCO will endeavor to represent IC supportability capabilities and concerns to the greatest extent possible. When intelligence support requirements and issues exceed the expertise of J-283/IRCO personnel, a recommendation will be made to grant access to applicable SME(s) for a more comprehensive document review, and transmittal of intelligence certification memoranda will be conducted via appropriate communications means.

4.8. Conditional Intelligence Certification.

4.8.1. When capability documentation has received threat approval from DIA, but does not adequately identify support requirements in one or more categories, J-283/IRCO may issue a conditional intelligence certification, allowing the capability to continue development while shortfalls are addressed. These shortfalls can often be resolved by including information from other capability documentation, such as PPP or LMDP, providing evidence of vulnerability assessments, or by documenting intelligence supportability assessments.

4.8.2. J-238/IRCO will coordinate with the Joint Staff Gatekeeper and Sponsor to determine if the capability can meet minimum standards in a reasonable period. Conditional certification will be valid for a specified period and may include periodic reviews with the Sponsor.

4.8.2.1. Conditional intelligence certifications will specify shortfalls and required conditions to be met for final certification. Once conditions have been satisfied, J-238/IRCO will issue a final intelligence certification; otherwise, J-238/IRCO, in consultation with the Lead FCB, will revoke the conditional intelligence certification in a memorandum provided to the Joint Staff Gatekeeper for distribution to DJ-8, the Sponsor, and Lead and Supporting FCBs.

4.9. Intelligence Certification Failure.

4.9.1. If J-283/IRCO determines that there are critical comments concerning intelligence that remain unsatisfactorily adjudicated, J-283/IRCO will recommend withholding intelligence certification for the capability requirements document to the certifying authority.

4.9.2. If the certifying authority concurs with J-283/IRCO's assessment, the intelligence certification shall be withheld until all critical comments

concerning intelligence have been adjudicated to the satisfaction of the commenter and J-283/IRCO.

4.10. Revocation of Intelligence Certification. When an organization or agency submits critical comments after the review period, or other circumstances arises that necessitate further review, J-283/IRCO may issue a letter revoking the current certification and provide to the Joint Staff Gatekeeper for distribution to DJ-8, the Sponsor, and Lead and Supporting FCBs. Once the review of comments or circumstances is complete, J-283/IRCO will reissue the intelligence certification.

ANNEX H TO APPENDIX G TO ENCLOSURE B
WEAPONS SAFETY GUIDE

1. Overview. This guide provides the policies and procedures for the weapon safety review and endorsement of weapons-related capability requirements documents. The endorsement ensures capability requirements documents adequately address the weapon safety requirements necessary for munition lifecycle management, including the safe use in the joint operating environment, as well as packing, handling, storage, transportation, and destruction/de-mil.

1.1. Purpose. The purpose of this appendix is to provide Sponsors with a content and endorsement guide for the Weapons Safety Endorsement (WSE) as part of the JCIDS process.

1.2. Applicability. This guide applies to munitions as defined in Title 10 U.S.C. § 101. In addition, the weapon safety assurance is applicable to directed energy weapons (DEW), EM rail guns, and all firing, launching, safety critical software, and controlling systems as part of the definition. Exceptions include nuclear weapons and their components; small arms and associated ammunition not containing electronics or software; intercontinental ballistic missiles; and space launch vehicles.

1.3. Proponent. The proponent for the WSE is the Protection FCB. For questions, contact the Protection FCB at (703) 693-7116. The JWSTAP also provides subject matter expertise to Sponsors for review during development of weapons program capability requirements documents prior to formal submission to the JCIDS process for review and validation.

2. Weapons Safety Content Guide. This guide provides document Sponsors with content related to the weapon safety assurance sections of CDDs. Weapon safety assurance is also applicable to weapon related DCRs to ensure that non-materiel solutions using an existing system do not introduce new safety issues, hazards, or risk as a result of the proposed changes.

2.1. Weapon system requirements.

2.1.1. Designation of weapons as joint systems. Because all weapons/weapons systems have the potential of being deployed together or employed in joint environments, weapons and weapons systems will be considered joint systems within the JCIDS process and may be designated as JROC or JCB Interest.

2.1.2. Tailoring of Weapon Safety Requirements. The guide provides standardized requirements for weapon safety, which Sponsors may propose to tailor depending upon the operational context in question.

2.1.2.1. In cases where a capability solution described in a CDD is intended to meet all baseline weapon safety requirements and criteria outlined above, and

no tailoring of weapon safety requirements are needed to address unique aspects of the operational context, the weapon safety assurance section of the CDD may state that fact.

2.1.2.2. In cases where tailoring of one or more of the baseline weapon safety requirements is proposed due to unique aspects of the operational context, the weapon safety assurance section of the CDD shall provide the weapon safety requirements which deviate from the standards. The Sponsor shall provide rationale for the deviations, traceable to the joint or multinational mission environment, and articulate the attributes and performance parameters that must be met as the basis for increased or decreased weapon safety requirements.

2.2. Baseline Weapon Safety Requirements.

2.2.1. System Safety. Reference [5] provides risk acceptance criteria for high, serious, medium, and low risks. Sponsors will identify the acceptable risk levels for weapon safety assurance. System safety and acceptable risk requirements informs the development of a System Safety Program (SSP) for the lifecycle of the weapon system IAW References [9] and [110].

2.2.2. Insensitive Munitions (IM): Standardized IM test protocols used in assessing a weapon's response to unplanned threats are established in References [111] and [112].

2.2.3. Fuse Safety. Fuse safety requirements are established in References [113], [114], and [115].

2.2.4. Explosive Ordnance Disposal (EOD). Requirements for disposal of munitions containing or delivering energetic materiel must satisfy the EOD RDT&E authority IAW Reference [116]. Requirements for disposal will inform the development of a demilitarization and disposal plan IAW with treaties, international agreements, Federal and state regulations and laws, and Reference [5].

2.2.5. Laser Safety. If the munitions contain lasers, to protect and mitigate the risk to personnel from laser radiation to an acceptable level, requirements for engineering design, protective equipment, administrative controls, or a combination thereof are established in Reference [70].

2.2.6. E3 Ordnance Safety. E3 ordnance safety requirements are established in References [117] and [118], including but not limited to hazards of electromagnetic radiation to ordnance, electrostatic discharge, EMP, electromagnetic interference, electromagnetic vulnerability, lightning, and precipitation-static.

2.2.7. Weapon Packing, Handling, Storage, and Transportation: Safety standards for packing, handling, storage, and transportation are established in Reference [119].

2.2.8. Other Considerations. In addition to criteria in the categories above, Sponsors should consider criteria shown in Figure B-27.

Additional Weapon Safety Criteria	
• Joint and Service unique safety requirements	• Interoperability
• Service and Joint Concepts and/or CONOPS	• Software safety
• Assembly	• ESOH
• Disassembly	• Future CONOPS possibilities
• Maintenance	• HSI
• Testing	• Coalition factors
• Use	• Cultural factors

Figure B- 27: Safety Review Criteria

3. Weapons Safety Endorsement. This guide provides procedures to engage the JWSTAP, established IAW Reference [46], as a source of expert consultation regarding weapon safety within the joint operating environment for document Sponsors and the J-8/DDFP. The JWSTAP will collaborate with program Sponsors and the J-8/DDFP to develop possible solutions to weapon safety issues. Consultation in the development and review of capability requirements documents may be both prior to formal submittal into the JCIDS process and during the staffing process.

3.1. Weapon Safety Review.

3.1.1. These reviews will focus on identifying potential safety issues resulting from munition lifecycle management, including interactions between the proposed weapon and the joint operating environment, handling, packaging, transportation, destruction/de-mil, assembly, disassembly, maintenance, testing, storage, and use of the weapon system.

3.1.2. The JWSTAP, on behalf of the J-8/DDFP and based on the information provided in the capability requirements document under review, accomplishes the following:

3.1.2.1. Identifies potential safety issues associated with the proposed capability requirements in joint warfighting environments.

3.1.2.2. Coordinates with the DoD Explosives Safety Board to coordinate with reviews conduced IAW Reference [47].

3.1.2.3. Develops recommended revisions to the document language to reduce or eliminate the identified safety concerns while maintaining the desired operational effectiveness.

3.1.2.4. Advises the J-8/DDFP and FCBs in support of a JROC review of the capability requirements document.

3.1.3. The JWSTAP provides to the J-8/DDFP a WSE recommendation for each reviewed program. A WSE is the means for documenting that weapons-related capability requirements documents provides for safe munition lifecycle management, including integration into the joint operating environment, identification of potential operational limits due to potential hazards when the

weapon is handled, stored, transported, assembled, disassembled, maintained, tested, destroyed/demilled, or used in the joint operating environment.

3.2. JWSTAP Review Process.

3.2.1. The JWSTAP safety review is a “top down” review that is primarily focused on the safety of a weapon used in the joint operating environment. The output of this review is a WSE recommendation memorandum deliverable to the J-8/DDFP.

3.2.1.1. The JWSTAP will meet at the request of the JWSTAP Chair to conduct technical safety reviews of weapons related JCIDS documents, discuss items of mutual interest, develop WSE recommendations, and recommend policies and priorities to the J-8/DDFP related to the WSE process.

3.2.1.1.1. Travel to accomplish routine review actions shall be minimized to the extent feasible. Deliberations of the JWSTAP will be accomplished by electronic means to the maximum extent possible.

3.2.1.1.2. Funding to support JWSTAP activities, including travel and per diem costs, will be provided by the participating agencies.

3.2.1.2. JWSTAP members may also consult with SMEs within their respective Services or organizations to develop safety comments that represent a Service/organization-wide, technically sound, well-reasoned position.

3.2.1.3. The JWSTAP Chair shall serve as the primary point of contact for coordination with external agencies. The Chair will notify members when formal document reviews are required, and will assign suspense dates to ensure JWSTAP recommendations are provided to the DDFP within established timeframes.

3.2.1.4. Comments are normally staffed via the KM/DS system and require that JWSTAP members have access to SIPRNET resources and email. JWSTAP members shall establish a SIPRNET account for email and to access the KM/DS system to facilitate reviews and comment submission as part of the JCIDS document review process.

3.2.2. In order to review documents from a joint warfighting perspective, reviewers must understand the applicable Service and Joint Concepts and/or CONOPS. This can be accomplished by reviewing the DoDAF architecture views referenced in the capability requirements document. Reviewers can also gain greater understanding of the Service and Joint Concepts and/or CONOPS by referring to the ISP associated with the program, which defines the system operation, the interfaces, the environment, and the required support.

3.2.3. The JWSTAP safety review considers compliance with established standards, or the justification for deviations based upon unique operational context for the weapon:

3.2.3.1. System Safety. Is the Sponsor proposing compliance with system safety standards identified in this annex, or are proposed deviations justified in light of the operational context?

3.2.3.2. IM. Is the Sponsor proposing capability to resist unplanned threats per established standardized IM test protocols identified in this annex? If munitions are proposed to not meet all IM passing criteria, are proposed deviations justified in light of the operational context? Has the Sponsor provided details of and a proposed path forward for improving IM response, for consideration during review for the WSE? Status and plans for improving IM response are to be submitted for JROC approval using the IM strategic planning process.

3.2.3.3. Fuse Safety. Is the Sponsor proposing compliance with fuse safety standards identified in this annex, or are proposed deviations justified in light of the operational context?

3.2.3.4. EOD. Is the Sponsor proposing compliance with EOD standards identified in this annex, or are proposed deviations justified in light of the operational context?

3.2.3.5. Demilitarization and Disposal. If the munitions contain or deliver energetic materiel, is the Sponsor proposing compliance with treaties, international agreements, Federal and state regulations and laws, and Reference [5] in a demilitarization and disposal plan, or are proposed deviations justified in light of the operational context?

3.2.3.6. Laser Safety. Is the Sponsor proposing compliance with laser safety standards identified in this annex, or are proposed deviations justified in light of the operational context?

3.2.3.7. E3 Ordnance Safety. Is the Sponsor proposing compliance with E3 ordnance safety standards identified in this annex, or are proposed deviations justified in light of the operational context?

3.2.3.8. Weapon Packing, Handling, Storage, and Transportation. Is the Sponsor proposing compliance with packing, handling, storage, and transportation standards identified in this annex, or are proposed deviations justified in light of the operational context?

3.2.3.9. Other. Are other criteria specified by the Sponsor, or lacking thereof, appropriate to weapon safety in the operational context?

3.2.4. Each JWSTAP member will submit to the JWSTAP Chair, via the SIPRNET and using a standard CRM, the suggested changes to be incorporated in the JCIDS document that will eliminate or mitigate the safety concerns. IAW the CRM, the JWSTAP members shall identify the comment type (critical, substantive, or administrative) and rationale for each suggested change to the JCIDS document. Comments will be submitted by the suspense date specified by the JWSTAP Chair.

3.2.5. The JWSTAP shall strive for a unanimous position on formal JCIDS document reviews. In the event the JWSTAP cannot achieve agreement, the Chair may request a vote in order to resolve the matter. Each JWSTAP member shall have one vote. In the case of a tie, the JWSTAP Chair shall cast the deciding vote. If a JWSTAP position is established by majority vote, the minority opinion and rationale will be documented in the WSE recommendation memorandum submitted to the J-8/DDFP.

3.2.6. To document the results of the JWSTAP safety review, the JWSTAP Chair or Deputy provides a WSE recommendation memorandum to the J-8/DDFP, through the Chief, Joint Staff J-8 Force Protection Division (J-8/FPD). The memorandum will recommend one of the following:

3.2.6.1. WSE should be granted.

3.2.6.2. WSE, with limitations, should be granted.

3.2.6.3. WSE should be withheld.

3.2.7. In cases where the recommendation for a WSE is withheld or granted with limitations, the JWSTAP Chair will consolidate the suggested changes and the rationale and provide as two enclosures:

3.2.7.1. Enclosure (1) to the WSE recommendation memorandum identifies concerns with the JCIDS document under review in narrative format with supporting rationale.

3.2.7.2. Enclosure (2) to the WSE recommendation memorandum provides, in CRM format, the language to be incorporated in the document under review to eliminate the safety concerns. The J-8/DDFP will enter the recommendations and the supporting rationale into the KM/DS system for staffing.

3.2.8. WSE related comments will be returned to the Sponsor for adjudication along with other comments from the JCIDS staffing process. During the comment adjudication period, the Sponsor may consult with the JWSTAP to ensure that safety concerns are adequately addressed.

3.2.9. Following Sponsor comment adjudication, the J-8/DDFP will review the revised document, generate the WSE, and inform the Lead FCB that the WSE has been provided. If comments have not been adequately adjudicated, the J-8/DDFP will identify remaining issues for the Sponsor and notify the Lead FCB that the WSE will not be granted on the nominal timeline and recommend that the document not be forwarded for validation until issues have been resolved.

3.2.10. Safety Review Guidelines and Timelines. The JWSTAP safe weapons review will be conducted within the 21-day staffing timeline for JCIDS document reviews as outlined in this manual. Following Sponsor comment adjudication, the WSE will be provided within 7 days unless there are outstanding issues that the Sponsor did not address during comment adjudication. See Figure B-28.

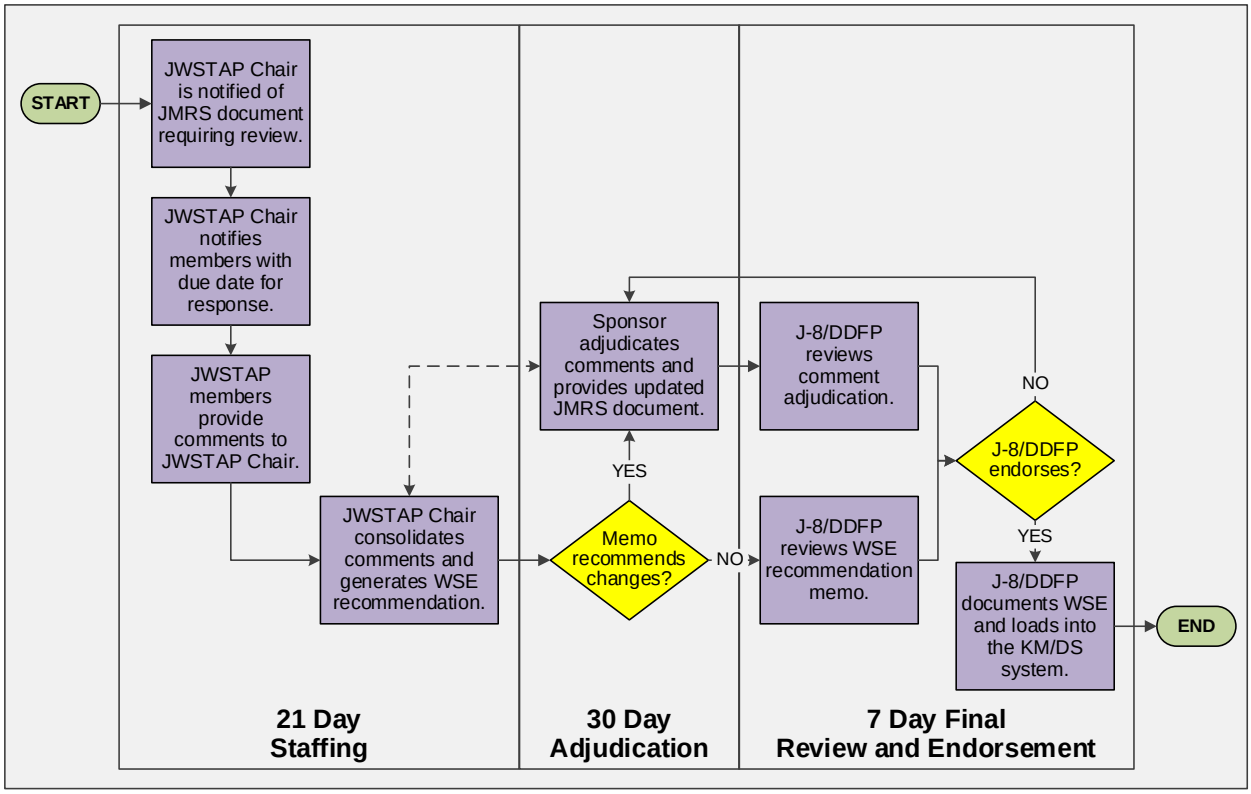

Figure B- 28: JWSTAP Process

APPENDIX H TO ENCLOSURE B

DoDAF PRIMER

1. Overview.

1.1. Purpose. This appendix provides a basic overview of the DoDAF and viewpoints that are pertinent to the JCIDS process.

1.2. Applicability. The DoDAF views described in this appendix apply to the JCIDS documents as specified in the individual document sections of Enclosure B to this manual.

1.3. Proponent. The proponent for this appendix is J-8/JCD. For questions, contact J-8/JCD at (703) 695-2705.

2. DoDAF Overview.

2.1. Description. DoDAF is the overarching, comprehensive framework and conceptual model enabling the development of architectures to facilitate DoD managers at all levels to make key decisions more effectively through organized information sharing across Department, JCA, Component, and Program boundaries. For JCIDS, DoDAF supports the following core processes:

2.1.1. Operations planning, including the operational contexts that serve as the basis for deriving capability requirements and identifying capability gaps.

2.1.2. Review and validation of capability requirements and associated capability gaps via the JCIDS process, including management of the capability requirements portfolios.

2.1.3. Approval of acquisition activities and milestones via the DAS process, including associated systems engineering and test/evaluation activities related to the capability solutions.

2.1.4. Supporting resource decision making in the Planning, Programming, Budgeting, and Execution (PPBE) process, including more robust traceability between the missions, capability requirements, and capability solutions supported by the resources.

2.1.5. For a more in-depth discussion of DoDAF, see Reference [6].

2.2. Architecture Repository. See References [7] and [112] for information about the federated architecture repository that enables access to architecture data and associated viewpoints from a wide variety of sources.

3. Architecture Products. DoDAF has several basic categories of viewpoints as illustrated in Figure B-29, which are further supported by models that capture data related to the overall viewpoint.

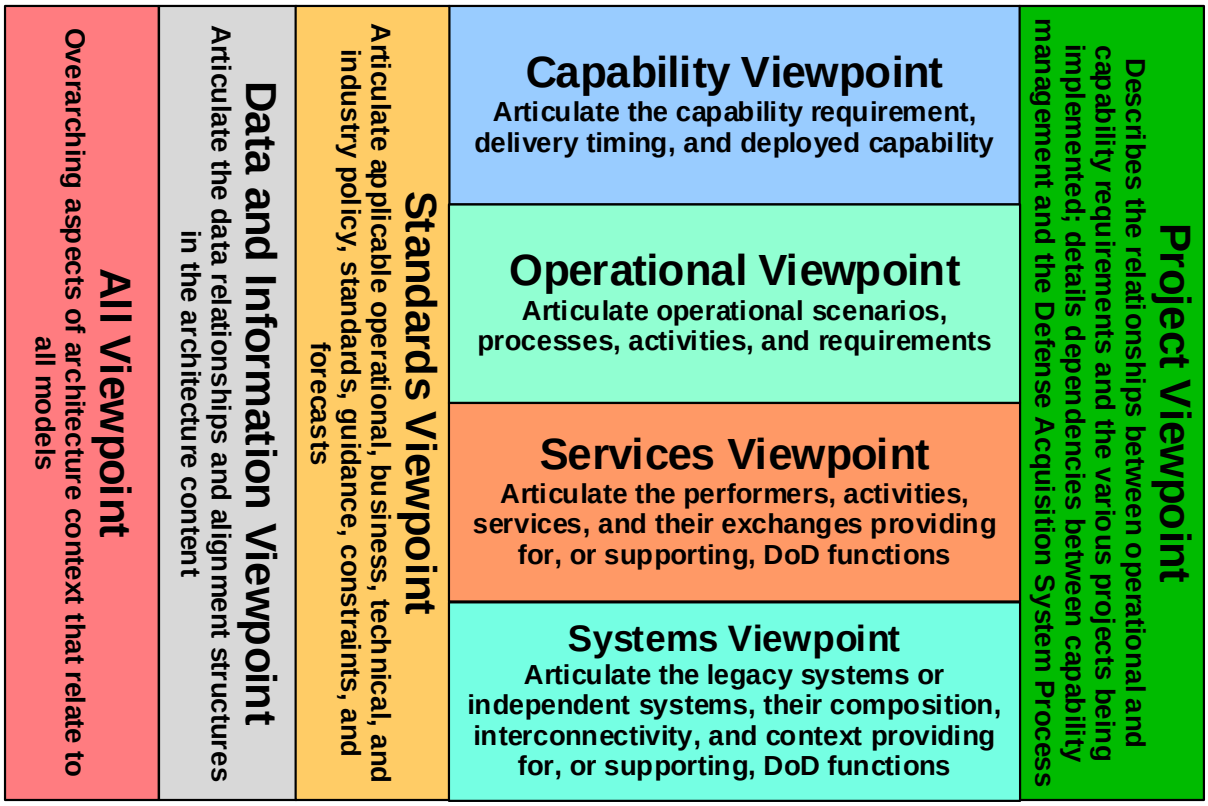

Figure B- 29: DoDAF Viewpoints

3.1. All Viewpoint (AV).

3.1.1. AV-1. Overview and Summary Information. Describes a Project's Visions, Goals, Objectives, Plans, Activities, Events, Conditions, Measures, Effects (Outcomes), and produced objects.

3.1.2. AV-2. Integrated Dictionary. An architectural data repository with definitions of all terms used throughout the architectural data and presentations.

3.2. Operational Viewpoint (OV).

3.2.1. OV-1. High-Level Operational Concept Graphic. The high-level graphical/textual description of the operational concept.

3.2.2. OV-2. Operational Resource Flow Description. A description of the Resource Flows exchanged between operational activities.

3.2.3. OV-3. Operational Resource Flow Matrix. A description of the resources exchanged and the relevant attributes of the exchanges.

3.2.4. OV-4. Organizational Relationships Chart. The organizational context, role, or other relationships among organizations.

3.2.5. OV-5.

3.2.5.1. OV-5a. Operational Activity Decomposition Tree. The capabilities and activities (operational activities) organized in a hierarchal structure.

3.2.5.2. OV-5b. Operational Activity Model. The context of capabilities and activities (operational activities) and their relationships among activities, inputs, and outputs; Additional data can show cost, performers, or other pertinent information.

3.2.6. OV-6.

3.2.6.1. OV-6a. Operational Rules Model. One of three models used to describe activity (operational activity). It identifies business rules that constrain operations.

3.2.6.2. OV-6b. State Transition Description. One of three models used to describe operational activity (activity). It identifies business process (activity) responses to events (usually, very short activities).

3.2.6.3. OV-6c. Event-Trace Description. One of three models used to describe activity (operational activity). It traces actions in a scenario or sequence of events.

3.3. Capability Viewpoint (CV).

3.3.1. CV-1. Vision. Addresses the enterprise concerns associated with the overall vision for transformational endeavors and thus defines the strategic context for a group of capabilities.

3.3.2. CV-2. Capability Taxonomy. Captures capability taxonomies. The model presents a hierarchy of capabilities. These capabilities may be presented in context of a timeline – i.e., it can show the required capabilities for current and future capabilities.

3.3.3. CV-3. Capability Phasing. The planned achievement of capability at different points in time or during the relevant periods of time. The CV-3 shows the capability phasing in terms of the activities, conditions, desired effects, rules complied with, resource consumption and production, and measures, without regard to the performer and location solutions.

3.3.4. CV-4. Capability Dependencies. The dependencies between planned capabilities and the definition of logical groupings of capabilities.

3.3.5. CV-5. Capability to Organizational Development Mapping. The fulfillment of capability requirements shows the planned capability deployment and interconnection for a particular capability phase. The CV-5 shows the planned solution for the phase in terms of performers and locations and their associated concepts.

CV-6. Capability to Operational Activities Mapping. A mapping between the required capabilities and the operational activities that those capabilities support.

3.3.6. CV-7. Capability to Services Mapping. A mapping between the capabilities and the services that these capabilities enable.

3.4. Project Viewpoint (PV).

3.4.1. PV-1. Project Portfolio Relationships. It describes the dependency relationships between the organizations and projects and the organizational structures needed to manage a portfolio of projects.

3.4.2. PV-2. Project Timelines. A timeline perspective on programs or projects, with the key milestones and interdependencies.

3.4.3. PV-3. Project to Capability Mapping. A mapping of programs and projects to capabilities to show how the projects and program elements help to achieve a capability.

3.5. Systems Viewpoint (SV).

3.5.1. SV-1. Systems Interface Description. The identification of systems, system items, and their interconnections.

3.5.2. SV-2. Systems Resource Flow Description. A description of Resource Flows exchanged between systems.

3.5.3. SV-3. Systems-Systems Matrix. The relationships among systems in a given Architectural Description. It can be designed to show relationships of interest, (e.g., system-type interfaces, planned vs. existing interfaces).

3.5.4. SV-4. Systems Functionality Description. The functions (activities) performed by systems and the system data flows among system functions (activities).

3.5.5. SV-5.

3.5.5.1. SV-5a. Operational Activity to Systems Function Traceability Matrix. A mapping of system functions (activities) back to operational activities (activities).

3.5.5.2. SV-5b. Operational Activity to Systems Traceability Matrix. A mapping of systems back to capabilities or operational activities (activities).

3.5.6. SV-6. Systems Resource Flow Matrix. Provides details of system resource flow elements being exchanged between systems and the attributes of that exchange.

3.5.7. SV-7. Systems Measures Matrix. The measures (metrics) of Systems Model elements for the appropriate timeframe(s).

3.5.8. SV-8. Systems Evolution Description. The planned incremental steps toward migrating a suite of systems to a more efficient suite, or toward evolving a current system to a future implementation.

3.5.9. SV-9. Systems Technology & Skills Forecast. The emerging technologies, software/hardware products, and skills that are expected to be available in a given set of time frames and that will affect future system development.

3.5.10. SV-10.

3.5.10.1. SV-10a. Systems Rules Model. One of three models used to describe system functionality. It identifies limitations that are imposed on systems functionality due to system design or implementation.

3.5.10.2. SV-10b. Systems State Transition Description. One of three models used to describe system functionality. It identifies responses of systems to events.

3.5.10.3. SV-10c. Systems Event-Trace Description. One of three models used to describe system functionality. It identifies system-specific refinements of critical sequences of events described in the Operational Viewpoint.

3.6. Data and Information Viewpoint (DIV).

3.6.1. DIV-1. Conceptual Data Model. The required high-level data concepts and their relationships.

3.6.2. DIV-2. Logical Data Model. The documentation of the data requirements and structural business process (activity) rules.

3.6.3. DIV-3. Physical Data Model. The physical implementation format of the Logical Data Model entities, e.g., message formats, file structures, physical schema.

3.7. Services Viewpoint (SvcV).

3.7.1. SvcV-1. Services Context Description. The identification of services, service items, and their interconnections.

3.7.2. SvcV-2. Services Resource Flow Description. A description of Resource Flows exchanged between services.

3.7.3. SvcV-3.

3.7.3.1. SvcV-3a. Systems-Services Matrix. The relationships among or between systems and services in a given Architectural Description.

3.7.3.2. SvcV-3b. Services-Services Matrix. The relationships among services in a given Architectural Description. It can be designed to show relationships of interest, (e.g., service-type interfaces, planned vs. existing interfaces).

3.7.4. SvcV-4. Services Functionality Description. The functions performed by services and the service data flows among service functions (activities).

3.7.5. SvcV-5. Operational Activity to Services Traceability Matrix. A mapping of services (activities) back to operational activities (activities).

3.7.6. SvcV-6. Services Resource Flow Matrix. It provides details of service Resource Flow elements being exchanged between services and the attributes of that exchange.

3.7.7. SvcV-7. Services Measures Matrix. The measures (metrics) of Services Model elements for the appropriate timeframe(s).

3.7.8. SvcV-8. Services Evolution Description. The planned incremental steps toward migrating a suite of services to a more efficient suite or toward evolving current services to a future implementation.

3.7.9. SvcV-9. Services Technology & Skills Forecast. The emerging technologies, software/hardware products, and skills that are expected to be available in a given set of timeframe and that will affect future service development.

3.7.10. SvcV-10.

3.7.10.1. SvcV-10a. Services Rules Model. One of three models used to describe service functionality. It identifies limitations that are imposed on systems functionality due to some aspect of system design or implementation.

3.7.10.2. SvcV-10b. Services State Transition Description. One of three models used to describe service functionality. It identifies responses of services to events.

3.7.10.3. SvcV-10c. Services Event-Trace Description. One of three models used to describe service functionality. It identifies service-specific refinements of critical sequences of events described in the Operational Viewpoint.

3.8. Standards Viewpoint (StdV).

3.8.1. StdV-1. Standards Profile. The listing of standards that apply to solution elements.

3.8.2. StdV-2. Standards Forecast. The description of emerging standards and potential impact on current solution elements, within a set of time frames.

4. Architecture Discovery and Accessibility.

4.1. Architecture Discovery. Architecture discovery is the first step in implementation of architecture information sharing and integration. Knowing where architecture products and data reside and having access to that information is critical to support architecture-based analysis processes. At a minimum, DoD Component architecture repositories will make each architecture project with its associated products (viewpoints) and architecture data sets discoverable to enterprise content search and discovery services.

4.2. Use of Enterprise Services. The Defense Information Systems Agency has requirements to provide enterprise services for Enterprise Content Search and Discovery (ECS&D), as well as cataloging information for discovery by DoD users. The WMA-AFIP leverages these services when available to ensure widest discovery and availability of Architecture content.

4.2.1. Architectures registered in the WMA-AFIP are automatically made discoverable to the enterprise search services.

4.2.2. Content registered with the catalog service is immediately discoverable to ECS&D services. When the URL points to document root, full text search functionality is enabled. Data can be loaded by:

4.2.2.1. Using DoD Discovery Metadata Specification (DDMS) compliant web services by either Simple Object Access Protocol or Representational State Transfer services.

4.3. Architecture Repository Types. For discovery of architecture content, the following three types of DoD Component architecture repositories have been identified:

4.3.1. An authoritative, database driven repository that is web-accessible. (e.g., Army Capability Architecture Development and Integration Environment).

4.3.2. An authoritative, non-database driven repository that is web-accessible (e.g., a SharePoint Portal).

4.3.3. An authoritative repository that is not web-accessible (e.g., shared drive, COTS tool environment, etc.).

4.3.4. Independent of type, the DoD Component is responsible for:

4.3.4.1. Ensuring all architectures and architecture related data developed by the Component are posted to the repository and made discoverable via enterprise services, and made accessible to external stakeholders.

4.3.4.2. Working with DoD CIO and appropriate mission area leads for delivery of structured data to support architecture based analysis requirements.

4.3.4.3. If existing repositories are not web-accessible, establishing processes and guidelines to make content of off-line repository web-enabled. Use of free enterprise tools such as Intelink/Inteldocs are a recommended option.

4.3.5. DoD Components with no authoritative repository. Organizations that fall under another DoD Component that has an established architecture repository will leverage that repository if feasible.

4.4. Accessibility of Architectures. Discovery of architectures does not ensure that the products and related data sets are accessible by users. Accessibility must be granted in a timely fashion to authorized users in order to support architecture-based analysis and decision-making processes.

4.4.1. NIPRNET Accessibility. In most NIPRNET environments basic Common Access Card (CAC) authentication is sufficient to protect unclassified artifacts. If special protection above basic CAC authentication is required, procedures for requesting access must be posted in a visible location and access must be granted to authorized users within 2 business days of request.

4.4.2. SIPRNET Accessibility. Public Key Infrastructure (PKI) Token authentication is in the process of widespread implementation on SIPRNET. If special protection above basic SIPRNET access or SIPRNET PKI Token authentication is required, procedures for requesting access must be posted in a visible location and access must be granted to authorized users within 2 business days of request.

5. WMA-AFIP.

5.1. WMA-AFIP Purpose. The purpose of the WMA-AFIP, located at the URL shown in Reference [7], is to provide a common context via a federated environment for sharing of WMA architecture, mission thread, and other related WMA capability integration information and data between various authoritative repositories in order to increase effectiveness and efficiency of decision-making in a dynamic environment by our customers.

5.1.1. WMA architecture information must conform to a level of compatibility in both data and structure to take advantage of data sharing services and the ability to analyze architecture data across the WMA Enterprise.

5.1.2. Development standards for WMA related architectures are available in Reference [7].

5.2. WMA-AFIP Lines of Effort.

5.2.1. Architecture Federation Methodology Development. The Joint Staff J-6, Deputy Director for Command, Control, Communications, Computers, and Cyber Integration (J-6/DDC5I) and architecture federation partners have developed methodologies and processes to support requirements for technical solution development (web services) of a federated architecture information sharing environment. This environment allows discoverability, accessibility, visualization, reuse, and traceability among various DoD-wide architecture repositories to support the following JCIDS related architecture information sharing needs:

5.2.1.1. Architecture products (DoDAF and Fit for Purpose views).

5.2.1.2. UJTL/JCA repositories (Joint Doctrine, Education, & Training Electronic Information System (JDEIS)).

5.2.1.3. JCIDS architecture documentation (i.e., KM/DS), DoDIN Technical Guidance – Federation and support for JCIDS architecture based analysis processes.

5.2.1.4. Process documentation/project architecture development.

5.2.1.5. Interoperability and capability requirements portfolio analysis of architecture data and associated artifacts/views.

5.2.1.6. Feedback and process improvement.

5.2.2. Technology Development: J-6/DDC5I and architecture federation partners will lead development of web-service enabled technical solutions to consume and expose baseline architectures and data from a federated set of architecture repositories. This includes:

5.2.2.1. Technology support for consumption of DoDAF Physical Exchange Specifications (PES) compliant web services and data.

5.2.2.2. Development of the service-oriented environment to support exposure of federated WMA architecture data and associated artifacts/views, products, analyses, and reports.

5.2.2.3. User interface design and development (standardized portal interface).

5.2.2.4. Support for architecture federation and information sharing with the Information Enterprise, Business, and Intelligence mission area Enterprise and Reference Architectures.

5.2.2.5. Support for WMA Mission Thread (MT) exposure and development to provide operational context.

5.2.2.6. Extract and convert architectures and associated data from various tools and converting to a reusable DoDAF format.

5.2.2.7. Provide technical support to standardize and expose architectures from stakeholders reliant on WMA Architecture Federation (support for legacy architectures that are not located in web-enabled environments).

5.2.3. Core Capability Support. Deployment and Maintenance of Production Environment. Support for the core capability and related services are essential to success. J-6/DDC5I is responsible for development and maintenance of processes and solutions to support:

5.2.3.1. Standardized portal interface maintenance and improvements.

5.2.3.2. Web service maintenance and improvements.

5.2.3.3. NIPRNET/SIPRNET production environment.

5.2.3.4. Cross-domain synchronization.

5.2.3.5. Configuration control/change management.

5.2.3.6. Federated architecture data management.

5.2.4. WMA Architecture Lexicon Development and Standardization. WMA architectures must achieve semantic understanding with DoD-level architectures and with adjacent architectures. The architecture data and associated artifacts/views must align within a common framework of semantic understanding based on the use of Component and mission area taxonomies or other mechanisms aligned with the appropriate department level (e.g., Community of Interest (COI)/Community of Practice (CoP) common vocabularies or DoD-level taxonomies from capability or reference architectures). This type of alignment will support the required level of detail needed for technical analysis of capability gaps, overlaps, redundancies, interdependencies, and interoperability. This line of effort includes:

5.2.4.1. Synchronization and development of WMA architecture lexicons to support the WMA Enterprise Architecture, architecture development and federation points, aligned with the DoD IEA and Business and Intelligence mission areas.

5.2.4.2. WMA architecture lexicon maintenance.

ENCLOSURE C

CAPABILITY REQUIREMENTS PORTFOLIO MANAGEMENT

1. Overview.

1.1. Purpose. The purpose of capability requirements portfolio management is to:

1.1.1. Manage and prioritize capability requirements within and across the capability requirements portfolios.

1.1.2. Inform other assessments, processes, and activities within the Joint Staff and across DoD.

1.1.3. Enable the JROC and CJCS to meet their statutory responsibilities outlined in Reference [2].

1.2. Applicability. Guidance in this enclosure applies to all FCBs and the Joint Staff elements responsible for capability requirements portfolio management.

1.3. Proponent. The proponent for this enclosure is J-8/JCD. For questions, contact J-8/JCD at (703) 695-2705.

2. Capability Requirements Portfolio Management.

2.1. Capability requirements portfolios. Capability requirements portfolios are established using Joint Capability Areas (JCAs) as an organizing construct IAW Reference [1]. This provides the FCBs a common framework to manage their capability requirements portfolios that is functionally grouped to support capability analysis, strategy development, investment decisions, capabilities-based force development, and operational planning.

2.1.1. Capability requirements portfolios include capability requirements validated by the JROC/JCB/independent validation authority that follow either the deliberate or urgent/emergent process lanes IAW Enclosure A of this manual.

2.1.1.1. FCB responsibilities within a portfolio includes capability requirements with JCAs that fall under one FCB's portfolio as well as capability requirements that affect more than one FCB. For example, a system being reviewed by the Force Application (FA) FCB due to its primary capabilities, may also have radar/sensor capabilities which are applicable to the Battlespace Awareness (BA) FCB portfolio.

2.1.1.2. Sub-portfolios may be organized by the FCB Chairs in cases where the breadth of the capability requirements portfolio makes analysis and decision support efforts cumbersome without further subdivision.

2.1.1.3. Information related to validated capability requirements is available via KM/DS system at the URL in Reference [4], with additional information available from the wiki site at the URL in Reference [120].

2.1.2. Each validated capability requirement aligns with one of three categories shown in Figure C-1 and discussed below in subparagraphs (a), (b), and (c):

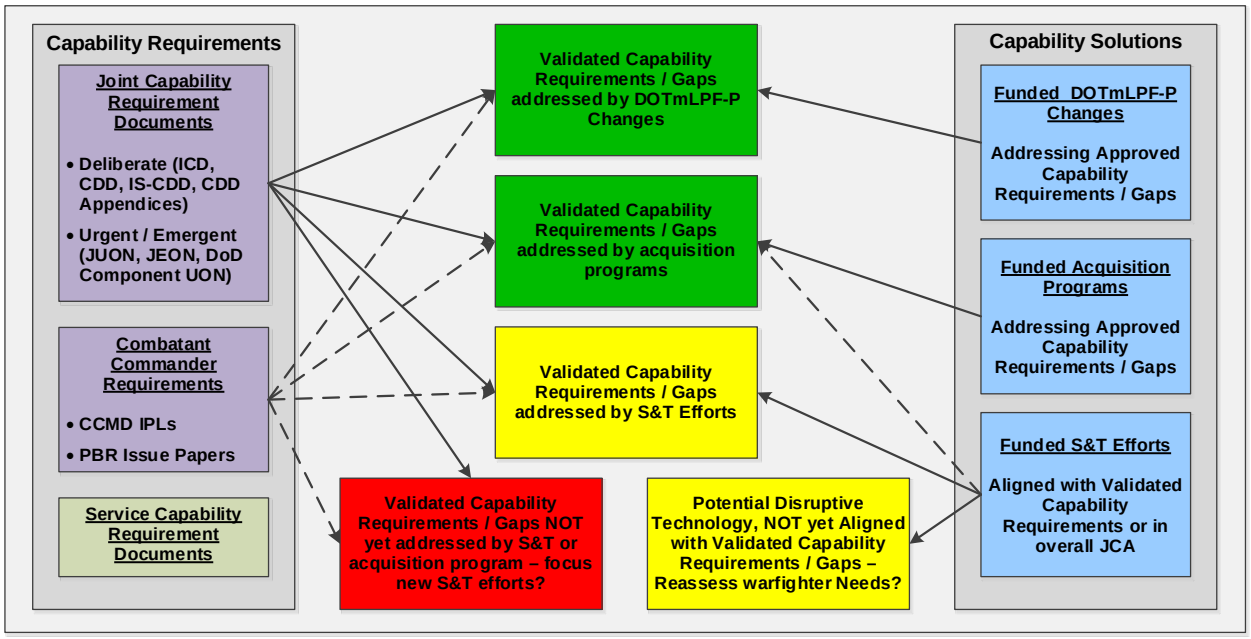

Figure C- 1: Notional Capability Requirements Portfolio

2.1.2.1. Validated capability requirements being addressed by an acquisition program or implementation of DOTmLPF-P changes. (Depicted by the information in the Green Bubbles in Figure C-1.)

2.1.2.1.1. FCBs and primary stakeholders maintain awareness of progress toward satisfying the validated capability requirements and ensure potential changes to programs or timelines are assessed for their impact on the capability requirements portfolio. FCBs also ensure that newly proposed capability requirements are not duplicative of efforts already underway.

2.1.2.1.2. S&T organizations maintain awareness of technology challenges within and across acquisition programs for potential alignment of S&T efforts.

2.1.2.1.3. Information related to acquisition programs is available via the Defense Acquisition Management Information Retrieval (DAMIR) system at the URL in Reference [121], or Sponsor equivalent databases. Information related to implementation of DOTmLPF-P changes resulting from validated Joint DCRs is available via the KM/DS system at the URL in Reference [4].

2.1.2.2. Validated capability requirements not yet addressed by an acquisition program or implementation of DOTmLPF-P changes, but aligned with ongoing or recently completed S&T efforts at TRL 3 or greater. Visibility into S&T efforts potentially addressing warfighter needs leverages a key aspect of the

DoD scientific and technical information program outlined in Reference [122]. (Depicted by the information in the Yellow Bubbles in Figure C-1)

2.1.2.2.1. FCBs and other stakeholders maintain awareness of S&T efforts potentially applicable to validated capability requirements to ensure proper advocacy for execution and timely transition of S&T efforts when applicable to satisfying validated capability requirements.

2.1.2.2.2. Program Managers (PMs) maintain awareness of S&T efforts where incorporation of technologies matured outside of acquisition programs could improve cost, schedule, and/or performance.

2.1.2.2.3. Information related to ongoing and recently completed S&T efforts is available via the Defense Technical Information Center's (DTIC) Unified Research and Engineering Database at the URL in Reference [123].

2.1.2.3. Validated capability requirements not yet being addressed by an acquisition program, implementation of DOTmLPF-P changes, or ongoing or recently completed S&T efforts. (Depicted by the information in the Red Bubble in Figure C-1)

2.1.2.3.1. S&T organizations maintain awareness of validated capability requirements for potential alignment of future S&T efforts.

2.1.2.3.2. Information related to validated capability requirements is available via the KM/DS system at the URL in Reference [4].

2.1.3. To enable technological innovation, FCBs and other stakeholders must maintain visibility into funded S&T efforts that align with the general capability requirements portfolio but not with any validated capability requirement, as shown in Figure C-1. This visibility can potentially enable disruptive technology changes through reassessment of validated requirements in light of emerging technologies.

2.1.4. Knowledge of past requirements, acquisition, budgetary decisions, and rationale is also critical for making informed decisions on the validation of new capability requirements or when conducting periodic assessments of the capability requirements portfolios.

2.1.4.1. This awareness includes information from the past several cycles of the CGA and PBR, and the rationale that was behind the recommendations and decisions.

2.1.4.2. Reassessment of the capability requirements portfolio, including potential changes to previous validation decisions to better close or mitigate capability gaps, may also be necessary to adapt to changing global context, threats, or strategic guidance. Decisions must be with awareness of how more recent context differs from that informing the original decisions.

2.1.4.3. In cases where programs developing capability solutions to satisfy validated capability requirements are reduced or cancelled, the FCBs and other

stakeholders must assess the impact on the capability requirements portfolios. See the JROC/JCB Tripwire review activities later in this enclosure.

2.1.5. Capability requirements and other issues that cross capability portfolios will be handled by teaming FCBs and other organizations.

2.1.5.1. For issues lying primarily within a Lead FCB and requiring support from one or more supporting FCBs, the Lead FCB will coordinate with the supporting FCBs as required.

2.1.5.2. For issues with significant crosscutting impact, leadership may designate J-8/JCD to coordinate analysis efforts, with participation from the appropriate FCBs, J-8/CAD, J-8/PBAD, and other stakeholders with equities in the issue under review.

2.1.5.3. The FCB O-6 and FCB GO/FO Integration Groups provide discussion forums for oversight of crosscutting issues prior to the JCB or JROC.

2.2. Capability Mission Lattice (CML). The CML, shown in Figure C-2 and described in the following paragraphs, provides an integrating construct for articulating the dependencies between capability requirements as well as the traceability between related processes and activities across the department.

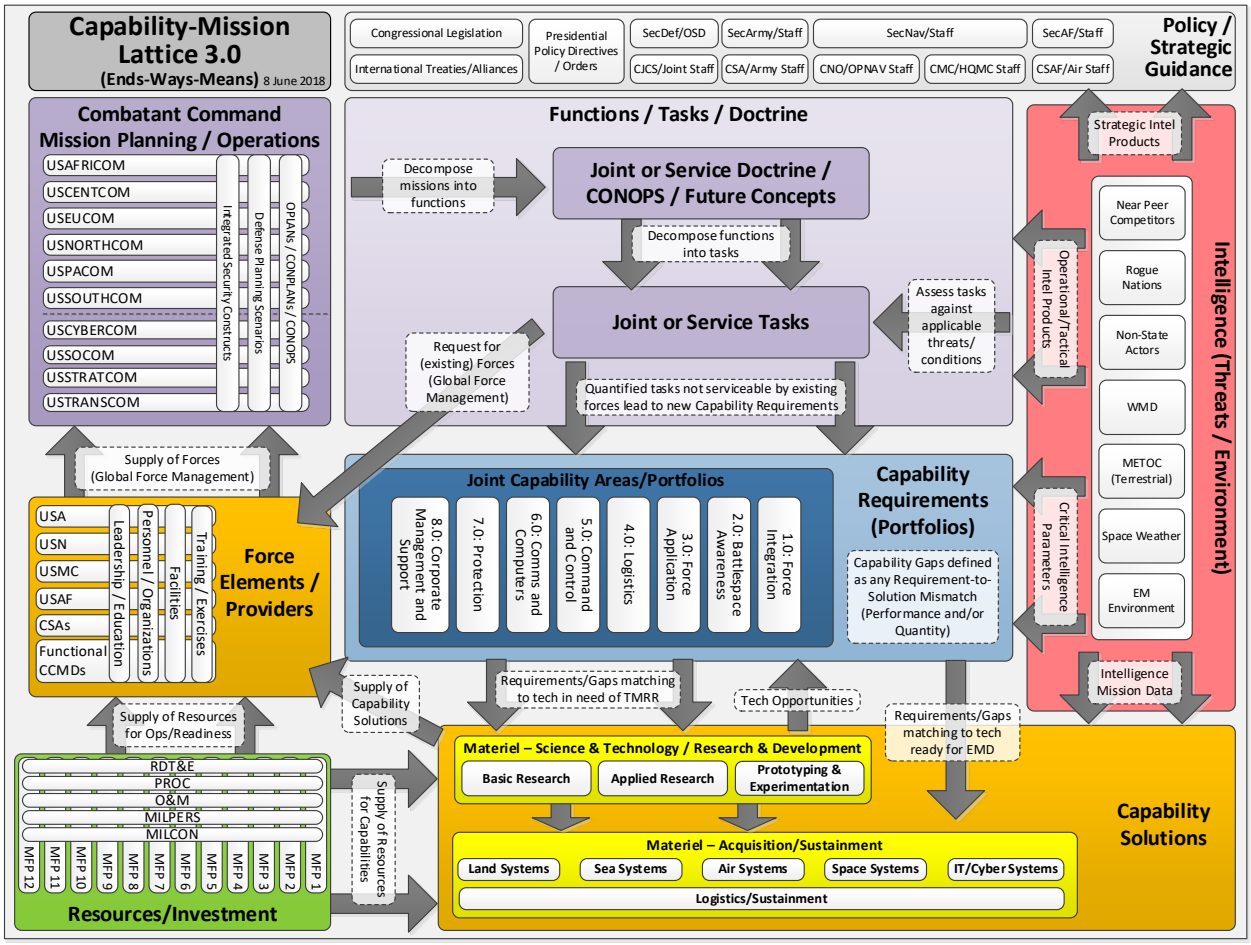

Figure C- 2: Capability-Mission Lattice (3.0)

2.2.1. Senior Leader Policy and Strategic Guidance. Guidance from many sources influences military operations, intelligence activities, development and validation of capability requirements, acquisition activities, and DOTmLPF-P associated with organizing, training, and equipping forces. It also influences the budgetary process that provides funding for these activities.

2.2.1.1. An organization's roles, missions, functions, tasks, or associated planning or operations must be consistent with senior leader policy and strategic guidance. Senior Leader policies and strategic guidance that is informed by intelligence guides Combatant Command mission planning and operations.

2.2.2. Intelligence (Threats/Environment). Intelligence activities identify and quantify threats that may drive or impact military operations, and the level of effectiveness needed to perform tasks, thus inform the setting of performance levels in capability requirements. The need to collect intelligence also drives capability requirements, often worked collaboratively between military and intelligence requirements processes when there are shared equities in the intelligence gathering capabilities.

2.2.3. Combatant Command Mission Planning/Operations. Current and planned operations, missions, and functions that direct an ability to perform certain activities are the most direct driver of capability requirements. Capability requirements associated with operations, which are not already available from the joint force, may result in capability gaps with associated operational risk if not mitigated by a new materiel or non-materiel capability solutions.

2.2.4. Functions/Tasks/Doctrine.

2.2.4.1. Joint Concepts, Service Concepts and CONOPS. These articulate how the organization plans to accomplish its roles, missions, or functions, which may be further decomposed into lower levels of the Universal Joint Task List (UJTL) or Service related tasks.

2.2.4.1.1. Joint Concepts. Joint Concepts within the Family of Joint Concepts (FoJC), identify a current or future military challenge and propose a solution to improve the ability of the joint force to address that military challenge.

2.2.4.1.2. Service Concepts, including USSOCOM, USCYBERCOM Concepts (within their Title 10 authority) and multi-Service Concepts, are written within the joint community to address focused, limited scope topics and may expand or implement ideas contained in Joint Concepts.

2.2.4.1.3. CONOPS. CONOPS articulate how the organization plans to accomplish its roles, missions, or functions, which may be further decomposed into lower levels of the Universal Joint Task List (UJTL).

2.2.4.2. While Sponsors may use other constructs, such as JMTs, kill chains, etc., to facilitate decomposition or assessment of their roles, missions, or functions, they must ultimately be captured in terms of tasks (e.g., UJTs and Service related). These lower level decompositions express the activities in terms of required operational capabilities to accomplish the activity.

2.2.5. Force Elements/Providers. The force providers - Services, USSOCOM, and Combat Support Agencies (CSAs) - organize, train, and equip using the materiel and non-materiel capability solutions available to provide ready forces to the CCMDs via the Global Force Management (GFM) process in Reference [124]. Readiness reporting of the force elements is performed IAW Reference [125] and [126].

2.2.6. Capability Requirements. Based upon strategic guidance, threats/intelligence, and military operations, the JROC, or an independent validation authority, reviews and validates proposed new capability requirements and performs periodic assessments of the capability requirements portfolios. Validated capability requirements which lack a materiel or non-materiel capability solution may be recommended for developing a new materiel or non-materiel capability solution to mitigate the operational risk associated with the capability gap.

2.2.7. Capability Solutions (Materiel and Non-Materiel).

2.2.7.1. New or existing materiel and non-materiel solutions are developed in order to ensure that the warfighter can meet the validated capability requirements and fill the associated capability gaps.

2.2.7.2. Rigorous analysis is conducted to determine the right mix of performance attributes and to ensure the right level of performance values are captured to ensure that the acquisition community develops or procures the right solution to fill the capability gap(s).

2.2.8. Resources/Investment. Execution of the processes or activities in all areas requires appropriate funding. The best justification for resources is to be able to articulate the interactions and traceability between each area of the CML, and how the resources buy down risk in capability, quantity, and/or readiness under mission/threat conditions.

3. Executing Capability Requirements Portfolio Management. FCB Chairs and other stakeholders must be advocates for changes to the capability requirements portfolio which are in the best interest of the joint force, and not necessarily advocate for every capability requirement proposed by Sponsors. They must ensure that the correct EA products are updated to reflect how new or modified capability requirements, and associated materiel and non-materiel capability solutions, impact their capability requirements portfolios without introducing unnecessary redundancy in capability or capacity. To facilitate capability requirements portfolio management, a number of periodic and event driven reviews may be applicable to each capability requirements portfolio.

3.1. Periodic Capability Reviews.

3.1.1. Capability Gap Assessment (CGA). The CGA is an annual assessment, coordinated by the J-8, which examines CCMD identified prioritized gaps as part of the Annual Joint Assessment. The CGA groups similar gaps, assesses efforts to close or mitigate capability gaps, and recommends programmatic and/or non-programmatic actions to close or mitigate capability gaps. See Appendix A to this enclosure for more detail of the CGA process.

3.1.2. Munitions Requirements Process (MRP). The MRP is an annual review of near-year and out-year total munitions requirements, IAW Reference [127], identifying total required munition inventories needed to enable execution of CCMD assigned missions. Analysis conducted as a part of MRP is a key aspect of managing the munitions portfolio and supporting capability requirement decision making.

3.1.3. Program and Budget Review (PBR). The PBR is an annual review coordinated by OUSD(C) and CAPE that facilitates consolidation of Program Objective Memorandum (POM) and Budget Estimate Submissions (BES) and adjudication of any outstanding issues from across the DoD before presenting the overall DoD input to the President's budget submission.

3.1.3.1. PPBE Process. For additional information on the PPBE process see Reference [128].

3.1.3.1.1. Planning. Planning examines U.S. defense posture in the global context, considering national security objectives and the need for efficient management of defense resources. The focus of planning is to define the NDS necessary to maintain national security and support U.S. foreign policy, and to provide the SecDef with strategic decision options. These options are informed by relevant Joint Operating Concepts and analysis of current and programmed forces in relation to the demands of the primary missions defined by the defense strategy. Results of the planning phase inform the development of proposed programs by the DoD Components.

3.1.3.1.2. Programming. DoD Components develop proposed programs, which in the aggregate form their POMs, consistent with planning guidance, programming guidance, and fiscal guidance. These programs reflect analysis of missions and objectives to be achieved, alternative methods of accomplishing them, and the effective allocation of resources. OSD conducts an annual PBR to adjudicate program and budget issues and better align the overall DoD budget prior to submission to OMB. The result of PBR is a Program Decision Memorandum (PDM), which directs changes to the POMs as they are consolidated into the overall DoD budget submission to OMB.

3.1.3.1.3. Budgeting. DoD Components develop and submit detailed budget estimates for their programs IAW fiscal guidance, programming guidance, and DoD financial management regulations in Reference [129]. A budget review is

conducted as part of PBR to ensure that programming and budgeting are aligned with the priorities of the joint force. Since the DoD budget is only a portion of overall government expenditures, OMB consolidates the budget submissions from all of the government departments and agencies, and produces the President's Budget for submission to Congress. Through a number of committees and legislative procedures, and informed by the President's Budget and testimony of various DoD officials, Congress authorizes and appropriates funds as it sees fit for the execution of DoD programs.

3.1.3.1.4. Execution Review. Using the funding provided by Congress, the Services, CCMDs, and other DoD Agencies execute their programs and interact directly or indirectly with the JCIDS process with activities including study, identification, validation of new capability requirements with associated capability gaps, development and acquisition of new capability solutions, and Operations and Support (O&S) of fielded capability solutions. The DoD Components conduct annual execution reviews to determine how well programs and financing have met joint warfighting needs.

3.1.3.2. Requirements context for PBR decision making.

3.1.3.2.1. Following POM/BES submissions, CAPE organizes issue teams as needed to review program issues, while the OUSD(C) conducts budgetary pricing, and execution reviews. Both CAPE and the OUSD(C) recommend potential adjudication for senior decision makers. Issue team membership includes representatives from across the Joint Staff and OSD as well as the DoD Components, to assure that joint equities are properly represented.

3.1.3.2.2. As close coordination of JCIDS, DAS, and PPBE processes is critical, the FCB Chairs, supported by representatives from the FCBs, J-8 JCD, J-8/CAD, and J-8/PBAD, participate in issue teams to provide the warfighter capability requirement perspective.

3.1.3.3. The PBR provides a key opportunity to ensure that budgetary decisions are fully informed by the priorities of the validated capability requirements of the joint force. Ongoing capability requirements portfolio management and prioritization, as well as the output of the most recent CGA and MRP provide essential context to discussions during PBR.

3.1.3.3.1. FCBs and other stakeholders also review issue papers submitted to PBR from other sources in the context of the impact they may have on the capability requirements and priorities within the capability requirements portfolios, dependencies within and across capability requirements portfolios, and potential impact on operational risk for the joint force.

3.1.3.3.2. At the end of PBR, as a result of the budgetary decisions made, assessments are to be updated to reflect the latest decisions relating to funding (or not) of capability solutions addressing the capability requirements within each capability requirements portfolio.

3.1.3.4. In cases where PBR directs funding be made available to address issues not already supported by validated capability requirements, the FCBs will provide recommendations to the JROC to facilitate Sponsor development of the appropriate capability requirements document for review and validation.

3.1.4. Capability Portfolio Management Review (CPMR). As needed, not to exceed annually, FCBs shall conduct a review of their capability portfolios to support DJ-8 in the determination of the Joint Staff Position for PBR or to inform other processes across the department including, the Chairman's Independent Risk Assessment (IRA). Guidance for each review will be provided, in writing, by DJ-8 to the FCB Chairs to initiate a CPMR.

3.1.5. Annual Review of Intelligence Mission Data (IMD) Prioritization. J-28 will lead an annual review (or as otherwise directed) of IMD requirements. This review will provide Joint Staff requirements input into IC production prioritization and provide an assessment of the residual risk to capability solutions based on production shortfalls.

3.1.6. Other capability requirements portfolio assessments. The FCB chairs also have responsibility for monitoring ongoing activities impacting their capability requirements portfolios, such as progress of AoA efforts and other acquisition activities, shortfalls in intelligence production, implementation of Joint Concepts, implementation of Joint DCRs, progress in satisfying JUONs, JEONs, and DoD Component UONs, etc. The FCB chairs may have the need to assess their capability requirements portfolios at other times throughout the year for a number of different reasons, including but not limited to:

3.1.6.1. The Vice Chairman of the Joint Chiefs of Staff (VCJCS) or other senior leadership may request an assessment of a capability requirements portfolio or sub-portfolio to inform their decision making on a topic, or to potentially identify new opportunities in a specific area.

3.1.6.2. The FCB chair may direct a capability requirements portfolio baseline assessment to better inform annual reviews such as CGA, PBR, or MRP.

3.1.6.3. A change in strategic guidance or other event may have such a significant impact on the content or priorities of a capability requirements portfolio that a reassessment is needed to adjust the focus of efforts related to that capability requirements portfolio.

3.1.7. Interactions with the Joint Strategic Planning System (JSPS). Management and prioritization of the capability requirements portfolios can provide robust support to, as well as be impacted by, activities of the JSPS outlined in Reference [130].

3.1.7.1. Annual Joint Assessment (AJA). This annual survey is used in part as the means by which the CCMDs provide their IPL inputs to initiate the annual CGA conducted IAW Reference [1] and this manual.

3.1.7.2. Joint Strategy Review (JSR). The JSR has several components which impact the management and prioritization of the capability requirements portfolios.

3.1.7.2.1. Joint Intelligence Estimate (JIE), Joint Strategic Assessment (JSA), and JSR Report. The JIE, JSA, and JSR provide important context for the evaluation of capability requirements portfolios and contribute to the left and right sides of the CML.

3.1.7.2.2. The Family of Joint Concepts (FoJC). The FoJC provides concept required capabilities and their associated implementation activities that can impact the management and prioritization of capability requirements portfolios. In turn, Joint Concept Development (JCD) Sponsors use AJA input and capability management portfolios for their baseline capability assessments and implementation plan development; identifying new or modified capability requirements for consideration in the JCIDS process. Details of the FoJC and JCD activities are in Reference [131].

3.1.7.2.3. Joint Logistics Estimate (JLE). The JLE evaluates how well the joint force can project, support, and sustain itself in the near-, mid-, and long-term, in support of the full range and number of missions called for in the NMS and JSCP. It must be informed by the capability requirements portfolio managed by the Logistics FCB, and may also identify new capability requirements and associated gaps for submittal into the JCIDS process.

3.1.7.2.4. Joint Personnel Estimate (JPE). The JPE evaluates how well the joint force develops and employs human capital over time, in support of the full range and number of missions called for in the NMS and JSCP. It must be informed by all stakeholders in Personnel issues in DOTmLPF-P across all capability requirements portfolios and may identify issues which impact the ability to fully implement and sustain capabilities in the capability requirements portfolios.

3.1.7.2.5. Chairman's Risk Assessment (CRA). The CRA is the CJCS' assessment of the nature and magnitude of strategic and military risk in executing the missions called for in the NMS, and may include recommendations for mitigating risk, including changes to strategy, development of new Service or Joint Concepts, evolving capabilities, increases in capacity, or adjustments in force posture or employment.

3.1.7.2.5.1. The CRA informs the review and validation of capability requirements in the capability requirements portfolios during normal staffing activities as well as during CGA, PBR, and other periodic reviews.

3.1.7.2.5.2. The CRA is also informed by the capability requirements and priorities in the capability requirements portfolios, and the acquisition activities underway to satisfy those capability requirements and reduce risk in conducting the missions called for in the NMS.

3.1.7.3.

3.1.7.4. Continuous Assessment Processes under JSPS.

3.1.7.4.1. Joint Combat Capability Assessment (JCCA). The JCCA is the near-term analysis of readiness and ability to execute required priority plans. It informs GFM sourcing decisions and CJCS risk assessments IAW Reference [132]. In cases where GFM cannot source the required capabilities and resulting risks are unacceptable, the JCCA may serve as the basis for quantity adjustments or new capability requirements being introduced into the JCIDS process.

3.1.7.4.2. Chairman's Readiness System (CRS). The CRS provides a common framework for conducting commanders' readiness assessments and enables leadership to gain greater visibility on readiness issues across the CCMDs, Services, and CSAs IAW References [125] and [126]. The CRS is also supplemented by CSA Review Team assessments performed IAW Reference [133].

3.1.7.4.3. GFM. The GFM process provides near term sourcing solutions while providing the integrating mechanism between force apportionment, allocation, and assignment IAW References [124] and [134] . In cases where GFM cannot source the required capabilities and resulting risks are unacceptable, the JCCA may serve as the basis for quantity adjustments or new capability requirements being introduced into the JCIDS process.

3.1.7.4.3.1. Interaction between the GFM and JCIDS processes is essential to ensure the optimum balance between validated capability requirements, force structure quantities, and allocation to address joint force priorities.

3.1.7.4.3.2. An instance of the GFM process not sourcing the forces requested does not necessarily imply that additional quantities of capability solutions are required, or that new capability requirements need to be submitted to the JCIDS process. However, significant or repetitive shortfalls in GFM sourcing may be reason to reassess capability requirements portfolios and, if required, adjust priorities and/or quantities of capability solutions.

3.1.7.4.4. Joint Force Sufficiency Assessment. Consists of two assessments – the GFMAP Sufficiency Assessment (GSA) and the Strategic Requirements Sufficiency Assessment (SRSA) (formerly known as the Joint Force Assessment) directed by the Global Force Management Implementation Guidance (GFMIG).

3.1.7.4.4.1. Process identifies all GFMAP shortfalls in a given fiscal year, develops recommended risk mitigating options, and informs other processes when appropriate.

3.1.7.4.4.2. The assessment considers both near-term sourcing issues and the future (end of the Future Years Defense Program (FYDP)) ability to execute the strategy. Results of the process do not address today's year-of-execution issues, rather, it illuminates gaps and provides option for senior leaders during the Program and Budget Review (PBR), the Global Force Management Board

(GFMB), informs the CGA process where practicable, and influences strategic guidance documents.

3.1.7.5. Chairman's Advice and Direction.

3.1.7.5.1. Chairman's Program Recommendation (CPR). The CPR provides the CJCS's personal recommendations to the SecDef, informs the Defense Planning Guidance (DPG), and influences resource decisions and development of the President's Budget.

3.1.7.5.1.1. The CPR articulates issues the CJCS deems important enough for the Secretary to consider when identifying DoD strategic priorities in the DPG. The CPR is informed by the annual CGA activities executed under the JCIDS process, and the assessment and prioritization of the capability requirements portfolios.

3.1.7.5.1.2. Since the CPR is personal correspondence to the SecDef, the document is not presented to the JCB and JROC for approval.

3.1.7.5.2. NMS. The purpose of the NMS is to prioritize and focus military efforts while conveying the Chairman's advice with regard to the security environment and the necessary military actions to protect vital national interests. The NMS provides military ends, ways, and means that inform development of the GEF and the development of joint force capabilities. As such, it serves as a key piece of strategic guidance when assessing and prioritizing the capability requirements portfolios.

3.1.7.5.3. JSCP. The JSCP provides guidance to accomplish tasks and missions based upon near-term military capabilities, and implements campaign, campaign support, contingency, and posture planning guidance reflected in the GEF.

3.1.7.5.3.1. Assessment and prioritization of the capability requirements portfolios must align with the guidance and assumptions of the JSCP.

3.1.7.5.3.2. The planning efforts executed under the JSCP may lead to identification of new or modified capability requirements, which may then be documented and submitted to JCIDS for review and validation.

3.2. Event Driven Capability Reviews.

3.2.1. Changes to validated capability requirements.

3.2.1.1. There may be cases where it is necessary to change performance attributes (KPPs, KSAs, and APAs), or other aspects of a validated capability requirements document, due to factors related to lifecycle cost, technology, production, development, or other issues that prevent meeting performance thresholds outside of the milestone reviews and CDD Updates as described in the deliberate JCIDS process.

3.2.1.2. When the JCB or JROC is the validation authority, except within the scope of change authorities delegated by the JCB or JROC to the Sponsor, the

Sponsor may request changes through the Joint Staff Gatekeeper. When a Sponsor proposes such a change, the updated document will be submitted for review and revalidation by the validation authority.

3.2.1.3. When the Sponsor is the validation authority, or acting within the scope of change authorities delegated by the JCB or JROC, the Sponsor may make changes as they deem appropriate. Within 14 days of validation, the Sponsor shall provide the updated document, with its associated change approval memorandum, to the Joint Staff Gatekeeper for archiving and visibility in the capability requirements portfolios.

3.2.1.4. Any changes potentially impacting certifications or endorsements will be reviewed by the applicable certification or endorsement authorities outlined in Enclosure A of this manual.

3.2.1.5. Changes to validated capability requirements documents will be assessed for operational risk and other impact on the management and prioritization of the capability requirements portfolios.

3.2.1.6. JROC/JCB Tripwire Reviews.

3.2.1.6.1. The JROC/JCB Tripwire review is a JCIDS activity for JROC and JCB Interest programs which enable re-examination of validated capability requirements, and the balance between performance levels and operational risk, to mitigate challenges in acquisition programs. Tripwire reviews are triggered by deviations from program costs, schedule, or quantity targets established at the time of validation.

3.2.1.6.1.1. The JROC/JCB Tripwire review applies to capability requirements identified in CDDs or IS-CDDs.

3.2.1.6.1.2. The JROC/JCB Tripwire review also applies in cases of program cancellation, as this represents an extreme case of schedule and quantity change.

3.2.1.6.2. In considering programs under JROC/JCB Tripwire review, the FCB chair and other stakeholders involved in the review and validation of the capability requirements evaluate the operational risk or other impact on the capability requirements portfolio and priorities if changes to cost, schedule, or quantity persist, or whether a lower level of one or more performance attributes (KPPs, KSAs, or APAs) can be accepted at reasonable risk or impact on help mitigate the trigger conditions.

3.2.1.6.3. The following trigger values apply unless tailored by the validation authority:

3.2.1.6.3.1. Cost. Programs must return to the JROC or JCB for revalidation if they experience a program cost growth equal to or greater than 10 percent over their current baseline or 25 percent over their original baseline as defined in the Acquisition Program Baseline (APB).

3.2.1.6.3.2. Schedule. Programs must return to the JROC or JCB for revalidation if they experience a schedule slip for IOC or FOC equal to or greater than 12 months from IOC and FOC targets set in the validation JROCM.

3.2.1.6.3.3. Quantity. Programs must return to the JROC or JCB for revalidation if they experience a reduction in operational inventory quantities equal to or greater than 10 percent from the quantity target set in the validation JROCM.

3.2.1.6.3.3.1. Changes to production quantities intended solely to accommodate unexpected attrition, or expenditure in the case of munitions and other expendables, and maintain the required operational inventory, do not trigger JROC/JCB Tripwire reviews and do not require revalidation.

3.2.1.6.3.3.2. Changes to production quantities which result in changes to the operational inventory, or lack of changes to production quantities necessary to maintain operational inventory when expenditure rates change, will trigger JROC/JCB Tripwire reviews, and require revalidation of required operational inventory quantities and/or acceptance of the altered operational risk.

3.2.1.6.4. See Enclosure A of this manual for details of the JROC/JCB Tripwire review process.

3.2.1.7. CIP Breach Review.

3.2.1.7.1. A CIP breach review is a collaborative assessment of the relationship between changes to an approved CIP - specific quantity, type, system capabilities, and technical characteristics or performance threshold of a foreign capability such as radar cross-section, armor type or thickness, or acoustic characteristics - and associated threat dependent capability requirements validated in ICDs, or for solution threat dependencies, associated performance attributes (KPPs, KSAs, and/or APA)s validated in CDDs.

3.2.1.7.2. The review is conducted by a risk mitigation team comprised of program office, capability Sponsor, capability developer, FCB representatives, and other applicable stakeholders.

3.2.1.7.3. When the supporting military Service Intelligence center determines an approved CIP was breached, notification of the breach will be made to appropriate offices in DoD, and the program office(s) and FCB(s) impacted by the breach.

3.2.1.7.4. The purpose of the CIP breach review is to:

3.2.1.7.4.1. Assess whether other current or future capability solutions, within the capability requirements portfolios, are impacted by the CIP breach.

3.2.1.7.4.2. Assess the impact of changes to adversary capabilities related to the approved CIP and determine if the breach compromises mission effectiveness of current or future capability solution(s).

3.2.1.7.4.3. Determine appropriate responses and/or risk mitigation efforts to balance potential increase in operational risk or costs with decisions to pursue (or not pursue) potential non-materiel and materiel changes.

3.2.1.7.5. CIP Breach Reviews use review procedures similar to Tripwire reviews, as shown in Enclosure A of this manual, but focusing on CIP parameter changes rather than cost, schedule, or quantity changes.

3.2.1.8. CICA.

3.2.1.8.1. CICA is similar to a CIP Breach Review in that it assesses the impact of classified information compromise against a capability portfolio. Compromised information may discuss performance parameters, technical specifications, capability gaps, or other aspects of the capability portfolio.

3.2.1.8.2. The review is conducted by a risk mitigation team comprised of program office, capability Sponsor, capability developer, FCB representatives, and other applicable stakeholders.

3.2.1.8.3. When the supporting military Service Intelligence center determines a compromise has occurred, they should notify the appropriate offices in DoD, and the program office(s) and FCB(s) impacted by the breach.

3.2.1.8.4. The purpose of the classified information compromise review is to:

3.2.1.8.4.1. Assess the impact of the compromise to changes to the effectiveness of current or future capability solution(s).

3.2.1.8.4.2. Assess whether other current or future capability solutions, within the capability requirements portfolios, are impacted by the compromise.

3.2.1.8.4.3. Determine appropriate responses and/or risk mitigation efforts to balance potential increase in operational risk or costs with decisions to pursue (or not pursue) potential non-materiel and materiel changes.

3.2.1.8.4.4. If there is a compromise of information that is not marked, but the total loss of that information is assessed as classified after the fact, it still falls under CICA standards.

3.2.1.8.5. Classified Information Compromise Reviews will use review procedures similar to Tripwire reviews, as shown in Enclosure A of this manual but focusing on the impact of the compromised information.

3.2.1.9. Nunn-McCurdy Unit Cost Breach Review.

3.2.1.9.1. The Nunn-McCurdy Unit Cost Breach review activity is an USD (A&S) process implemented to meet statutory review requirements in Reference [19]. More detail on Nunn-McCurdy Unit Cost Breach procedures are in Reference [5].

3.2.1.9.2. In considering programs under Nunn-McCurdy Cost Breach, the FCB chair and other stakeholders involved in the review and validation of the capability requirements evaluate the essentiality of the program to national security. For programs deemed essential to national security, they also

evaluate operational risk or other impact on the capability requirements portfolio and priorities from potential changes to one or more performance attributes, schedule, or quantity, if such a change would to help mitigate the unit cost breach conditions. See Enclosure A of this manual for details of JROC/JCIDS interaction with the Nunn-McCurdy Unit Cost Breach procedures.

3.2.1.10. Upgrades and end of service life decisions.

3.2.1.10.1. For incremental improvements to fielded capability solutions, through more capable production increments and/or retrofit of fielded systems, the Sponsor may use a new CDD or an appendix to a validated CDD. In this case, the Sponsor will staff and validate the proposed capability solution through the deliberate process as outlined in Appendix A to Enclosure A of this manual.

3.2.1.10.2. When a capability solution is approaching end of service life, there are three courses of action:

3.2.1.10.2.1. If the capability is obsolete or otherwise not required in the future, the validation authority will rescind the validation and the Sponsor will dispose of the capability solution. The capability requirements portfolio will be updated to reflect the removal of the capability requirements.

3.2.1.10.2.2. If the originally validated capability requirements remain valid, then a replacement capability solution can be acquired to meet the same performance attributes under the authority of the originally validated document. The capability requirements portfolio will be updated to reflect the replacement capability solution.

3.2.1.10.2.3. If adversary threats, strategic guidance, or other operational context have changed such that upgraded capabilities are required for the replacement system, a new capability requirements document will be generated by the Sponsor. FCB Chairs and other stakeholders will assess impact on the capability requirements portfolios during staffing of the document.

APPENDIX A TO ENCLOSURE C
CAPABILITY GAP ASSESSMENT

1. Overview.

1.1. Purpose. The CGA is a deliberate assessment by which the CJCS and JROC carry out statutory responsibilities outlined in References [2], [135], and [136]. Responsibilities supported by the CGA include:

1.1.1. Providing advice to the SecDef on the effect that critical force capability deficiencies and strengths will have on accomplishing national security objectives.

1.1.2. Providing advice on program recommendations and budget proposals to conform to priorities established for the CCMDs and in strategic plans.

1.1.3. Submitting to the congressional defense committees a report on the requirements of the CCMDs.

1.1.4. Conferring with and obtaining information from the CCMDs and evaluating and integrating that information into advice given to the President and the SecDef.

1.1.5. Assisting the SecDef with funding proposals for the CCMDs.

1.1.6. Identifying and assessing the priority of joint military requirements and assigning joint priority among fielded and future programs meeting valid requirements.

1.2. Applicability. This appendix applies to the Joint Staff, Services, CCMDs, and other DoD Agencies in situations as defined in the individual annexes. (Refer to the CGA Guide at Reference [137] for detailed information on the CGA process)

1.3. Proponent. The proponent for this appendix is J-8/JCD. For questions, contact J-8/JCD at (703) 695-2705.

2. Inputs to the CGA Process. The CGA process begins with the receipt of the IPLs provided by the CCMDs in response to the AJA and the Chairman's request for assessment of critical warfighter capability gaps linked to their top priority risk mitigation measures. Additional inputs include joint lessons learned, CDD needs, JUONs, JEONs, and Chief, National Guard Bureau (CNGB) issues. Since some inputs are received throughout the year, a "snapshot" of these inputs will be taken at the beginning of the CGA process to capture those issues to evaluate during assessment.

2.1. CCMD IPLs. Annually, the CCDRs submit a prioritized list of their most pressing capability gaps to the CJCS and the SecDef for inclusion in the Chairman's Annual Report to Congress. IPLs are intended to provide visibility for those few key problem areas which, in the judgment of the CCDR, require the highest priority attention by the DoD in finding capability solutions.

2.2. Capability requirements portfolio management. Throughout the year, FCBs conduct capability requirements portfolio management IAW this manual. As part of this function, they monitor and manage joint military requirements, capability gaps, and proposed capability solutions. All of these elements are essential to the CGA process and provide input into the CGA in the form of on-going efforts and assist in developing recommended actions for the CGA JROCM.

2.3. Joint Lessons Learned. Joint lessons learned, IAW Reference [138], are the discovery, validation, integration, evaluation, and dissemination of lessons from joint operations, training events, exercises, experiments, Title 10 wargames, and other activities in peacetime and war. Joint lessons learned influence the CGA process by identifying capability gaps with the goal of delivering the best military capability solutions in support of national security.

2.4. CNGB Issues. In response to the AJA, CNGB provide input to the CCMDs for inclusion in their IPLs high priority capability gaps, prioritized across Service and functional lines, risk area, and determining long-term strategic planning issues.

2.5. Non-CGA IPLs. Certain issues submitted within CCMD IPLs are not capability gaps and are outside the responsibilities of the JROC. Resolution or mitigation of these issues is handled outside the CGA process.

3. Capability Gap Assessment (CGA) (Reference [137]).

3.1. Initial Assessment and Assignment. Receipt of the IPLs from the CCMDs. The CGA provides a key opportunity to adjust and reprioritize capability requirements within each capability requirements portfolio to better serve the needs of the joint force, as articulated by the CCMDs in their IPLs.

3.1.1. CCMDs annually submit IPLs for capability requirements, assessed across DoD Component and functional lines, which represent capability gaps limiting CCMD assigned mission accomplishment.

3.1.2. Where appropriate, the output of the CGA will recommend mitigation strategies for the identified capability gaps which better prioritize the efforts to improve the capability requirements portfolios.

3.2. FCB Assessment. Assess CCMD entries against the NMS; assessment of on-going efforts, and complete risk assessment. The FCBs and other stakeholders involved in the CGA process must consider the priorities of the CCMDs in context of the capability requirements portfolios in present and future timeframes. Any potential mitigation strategies for a capability gap must also be considered in terms of its impact on other capabilities and dependencies within and across capability requirements portfolios. JS/J-7 Joint Concepts Division will provide the FCBs Joint Concepts' contribution to CCMD IPL mitigation for current and enduring force requirements through an assessment of concept required capabilities' activities.

3.3. Development of Recommended Actions. In cases where the CGA identifies new capability gaps that are not already supported by validated capability requirements, the FCBs will provide recommendations to the JROC to facilitate Sponsor development of the appropriate capability requirements document for review and validation.

APPENDIX B TO ENCLOSURE C
IDENTIFICATION OF JOINT MILITARY CAPABILITY REQUIREMENTS

1. Overview.

1.1. Purpose. The purpose of any approach outlined in this section is for a Sponsor to derive and refine joint military capability requirements and associated capability gaps – for which a capability solution must be provided either organically or leveraged through the joint force – to accomplish assigned functions, roles, missions, and operations.

1.1.1. Use of certified requirements managers. Sponsors will use certified requirements managers, as described in Enclosure D of this manual, to monitor and evaluate capability requirement identification, including but not limited to the identification of capability gaps due to changes in threats, missions, or aging of legacy weapon systems throughout their lifecycle.

1.1.2. Relation to functions, roles, missions, and operations. Before any action can be taken in the JCIDS process related to reviewing and validating capability requirements documents, Sponsors must first identify capability requirements related to their functions, roles, missions, and operations.

1.2. Applicability. This appendix applies to the Joint Staff, Services, CCMDs, and other DoD Agencies.

1.3. Proponent. The proponent for this appendix is J-8/JCD. For questions, contact J-8/JCD at (703) 695-2705.

2. Identifying Capability Requirements.

2.1. General Approach.

2.1.1. Sponsors may pursue a variety of approaches to determine their organizational capability requirements, depending upon the timeliness of the assessment and the scope of the activities being reviewed. Due to the wide array of issues that may be considered, the breadth and depth of each approach must be tailored to suit the issue. The approach must be sufficient to develop coherent and well-supported recommendations, which the validation authority will then use to validate the capability requirements and associated capability gaps to support possible follow-on actions.

2.1.2. While Sponsor activities may examine various aspects of their capability requirements in significant levels of detail, the key for JCIDS is to identify the high level operational capability requirements, establish quantifiable attributes and metrics, and articulate the traceability from those capability requirements to the tasks, missions, threats, and overall strategic guidance.

2.1.3. For each identified capability requirement, Sponsors then compare them to current and programmed future capability solutions, if any, to determine if there are any capability gaps which present an unacceptable level of risk and

warrant further development of materiel or non-materiel capability solutions to close or mitigate the capability gaps.

2.1.4. When the operational risks involved with not closing the capability gaps outweigh the potential resources associated with pursuing a capability solution and potential operational risks introduced by removing the resources from other efforts, the Sponsor may recommend the most appropriate path forward to satisfy the capability requirements and reduce or eliminate any associated capability gaps.

2.2. Leverage of prior efforts. The Sponsor must identify and build upon any previous CBAs, studies, and other analytical products applicable to the area of interest. In addition to analytic products available within the Sponsor's organization, previous studies may also be accessible through the KM/DS system at the URL in Reference [4]. The intent is to avoid any unnecessary repetition of prior efforts, and provide continuity between analyses for reviewers and decision makers. This does not preclude the Sponsor from applying different context or different assumptions, as appropriate for the approach being pursued.

2.3. Considerations. Any approach taken by a Sponsor must address the following areas:

2.3.1. Description of the mission and military problem being assessed.

2.3.2. Identification and assessment of prior CBAs, studies, and other analytical products applicable to the area of interest.

2.3.3. Identification of the tasks to be completed to meet the mission objectives.

2.3.4. Identification of the joint military capability requirements within one or more of the JCAs, described in terms of the tasks, performance, and conditions.

2.3.5. Assessment of capability gaps between the identified capability requirements and current or programmed capabilities across the joint force.

2.3.6. Assessment of operational risks associated with each capability gap if not addressed.

2.3.7. Evaluation of possible non-materiel and materiel approaches to satisfy part or all of the capability requirements and close or mitigate the associated capability gaps.

2.3.8. Evaluation of current and potential future S&T efforts which may enable a future capability solution, or future enhancements to current or proposed capability solutions.

2.3.9. Recommendation for the most appropriate approach to be taken to close or mitigate capability gaps and reduce operational risk.

2.3.10. Solution independence. The Sponsor is not to predetermine capability solution or end item, but instead provide data related to forms and functions of potential solutions to support the development of capability requirements documents. The final recommendations will include a focused and concise justification for the proposed action.

3. Primary Types of Approaches. Approaches for identifying joint capability requirements may include, but are not limited to:

3.1. Capabilities-Based Assessment.

3.1.1. The CBA provides an analytic basis to identify capability requirements and associated capability gaps prior to development and submission of capability requirements documents for review and validation.

3.1.1.1. Details of the CBA process are in Appendix A to Enclosure C and in References [139], [140], and [141].

3.1.1.2. Applicable Joint Concepts and associated implementation plans must be considered during CBAs and other analyses. Details of Joint Concept development activities are in Reference [131].

3.2. DOTmLPF-P Analysis. Analysis of DOTmLPF-P is part of all CBAs, but may be used independently of a CBA when the scope of an issue being studied is not likely to result in new materiel solution development.

3.2.1. Guidance for DOTmLPF-P considerations are found in Annex F to Appendix G to Enclosure B of this manual and in the references outlined in that annex.

3.2.2. The DOTmLPF-P Analysis generally results in one or more DCRs without an associated ICD.

3.2.2.1. DCRs which impact only the Sponsor organization may be reviewed, validated, and implemented IAW DOTmLPF-P policies and processes of that organization.

3.2.2.2. DCRs which impact multiple organizations typically lead to a Joint DCR for review and validation. Details of Joint DCRs are in Appendix E to Enclosure B of this manual.

3.3. Other Studies and Analysis. Organizations may conduct other forms of studies, analyses, or assessments which cover some aspects of what is typically covered in CBAs and DOTmLPF-P analysis. These other studies may be used as sources of capability requirements, but may need to be augmented or further refined through additional efforts before having sufficient data to properly quantify capability requirements and generate capability documents. Potential other processes and studies include, but are not limited to the following:

3.3.1. Operational Planning: Operational planning is performed IAW References [142], [143], [144], and [145].

3.3.1.1. Development of OPLANs and CONPLANs is one means to identify capability requirements related to CCMD roles and missions and the assignment or attachment of forces. Capability requirements identified during planning may require additional analysis as outlined for CBAs prior to submission of capability requirements documents for review and validation.

3.3.1.2. Planning for ongoing contingency operations may identify capability requirements which represent potential for critical mission failure or unacceptable loss of life if not satisfied in a compressed timeframe impractical to address with deliberate processes. These capability requirements may qualify for submission as JUONs or DoD Component UONs for expedited validation and rapid acquisition efforts in order to satisfy the validated capability requirement in the operational timeframe. Details of JUON documents are in Appendix F to Enclosure B of this manual.

3.3.1.3. Planning for anticipated contingency operations may identify capability requirements which represent potential for critical mission failure or unacceptable loss of life once operations commence, if not satisfied in a compressed timeframe impractical to address with deliberate processes. These capability requirements may qualify for submission as JEONs, or DoD Component UONs if Sponsor processes allow, for expedited validation and rapid acquisition efforts in order to satisfy the validated capability requirement in the operational timeframe. Details of JEON documents are Appendix F to Enclosure B of this manual.

3.3.2. Exercise/Warfighting Joint Lessons Learned. Warfighting and exercise joint lessons learned may serve as a basis to evaluate capability requirements if the documentation identifies that mitigation of capability gaps and reduction in operational risk is worth the required resources needed to implement the change. Joint lessons learned may require additional analysis as outlined for CBAs prior to development of capability requirements documents for validation in the deliberate or urgent/emergent staffing processes. See References [138] and [146] for more details of the joint lessons learned program.

3.3.3. JCTDs and other experiments. At a minimum, assessments of JCTDs and other completed experimentation must provide input that allows for a comprehensive analysis of the operational utility of the capability solution, and ultimately support a determination of whether there is a basis for establishing an enduring capability requirement. The scope of the assessment may be tailored depending upon the level of detail available to the Sponsor and the nature of the demonstrated capability solution.

3.3.3.1. An assessment may be a suitable replacement for analysis used as the basis for ICD or CDD preparation, depending upon the maturity of the capability solution. In these cases, assessments are to contain the critical elements of information that are described for CBAs and required in the capability requirements documents, including description of the capability requirements and associated gap(s); associated tasks, conditions, and

operational performance standards/metrics; and how the materiel and non-materiel approaches address these factors.

3.3.3.1.1. JCTDs or other prototypes tested in the field may serve as a basis to establish capability requirements, if an assessment indicates sufficient military utility of a demonstrated capability solution. More information on JCTDs is available from the JCTD Office in Reference [147].

3.3.3.1.2. Documentation of Joint or DoD Component experimentation may serve as a basis to establish capability requirements, if the documentation indicates sufficient military utility of a certain capability.

3.3.3.2. If the assessment does not provide sufficient detail to fully develop capability requirements documents, additional studies or analysis as outlined for CBAs may be used to complement the data available from the assessment.

3.3.4. Transition of Rapidly Fielded Capability Solutions.

3.3.4.1. JUONs, JEONs, and DoD Component UONs. Successful capability solutions for JUONs, JEONs, and DoD Component UONs may serve as a basis for validating enduring capability requirements to support transition of rapidly fielded capability solutions for sustainment and/or further development if they have a positive assessment of operational utility documented by the original requirement Sponsor.

3.3.4.2. See Appendix B to Enclosure A of this manual for details of assessments of operational utility for rapidly fielding capability solutions in support of JUONs and JEONs. An assessment for a capability solution initiated through a JUON or JEON does not need to duplicate information already contained in the validated JUON or JEON. However, the assessment may address refinements to the original capability requirements as needed to reflect knowledge gained from operating the rapidly fielded capability solution.

3.3.4.3. Assessment of successful DoD Component UONs intended for transition to enduring capability requirements is at the discretion of the Sponsor. Information to support the associated ICD or CDD for validation will be consistent with other guidance in this manual.

3.3.4.4. If the assessment does not provide sufficient detail to fully develop capability requirements documents, additional studies or analysis as outlined for CBAs may be used to complement the data available from the assessment.

3.3.5. Business Process Reengineering. Regardless of lifecycle cost, any IS other than a national security system, operated by, for, or on behalf of the DoD, including financial systems, financial data feeder systems, contracting systems, logistics systems, planning and budgeting systems, installations management systems, human resources management systems, training and readiness systems are considered DoD Business Systems.

3.3.5.1. DoD Business Systems support business activities such as acquisition, financial management, logistics, strategic planning and budgeting,

installations and environment, and human resource management, and generally are validated by the Business Capability Acquisition Cycle (BCAC), for business systems requirements and acquisition as outlined in Reference [37] and by the annual issuance of the CMO Defense Business Systems Investment Management Process Guidance, Reference [36]. Acquisition of DoD Business Systems uses capability requirements, information technology functional requirements and implementation plans to describe business systems requirements and establish objectives for their delivery. Formerly, problem statements and business case documents in lieu of ICDs and CDDs were used to document the capability requirements and associated capability solutions.

3.3.5.2. The Joint Staff representative to the DBC will perform an initial review and forward at his/her discretion, based on an assessment of business and warfighter equity, problem statements and business case documents to the Joint Staff Gatekeeper and appropriate FCB. In those cases where the Joint Staff Gatekeeper, on the advice of the appropriate FCB, determines that JCB or JROC oversight of the DoD Business System is required, the implementation plan, expressed in terms of releases and deployments, to describe business systems requirements and establish objectives for their delivery will be used in lieu of the typical capability requirements documents used in JCIDS staffing and validation. The implementation plan details development, delivery, and capability support plans for the business system and is sufficient for consideration on its own merits.

4. Determination of Appropriate JCIDS Action. A combination of actions may represent the most appropriate means of mitigating or closing the identified capability gap(s). Figure C-3 illustrates the typical JCIDS actions related to addressing capability gaps, which are detailed in the following paragraphs.

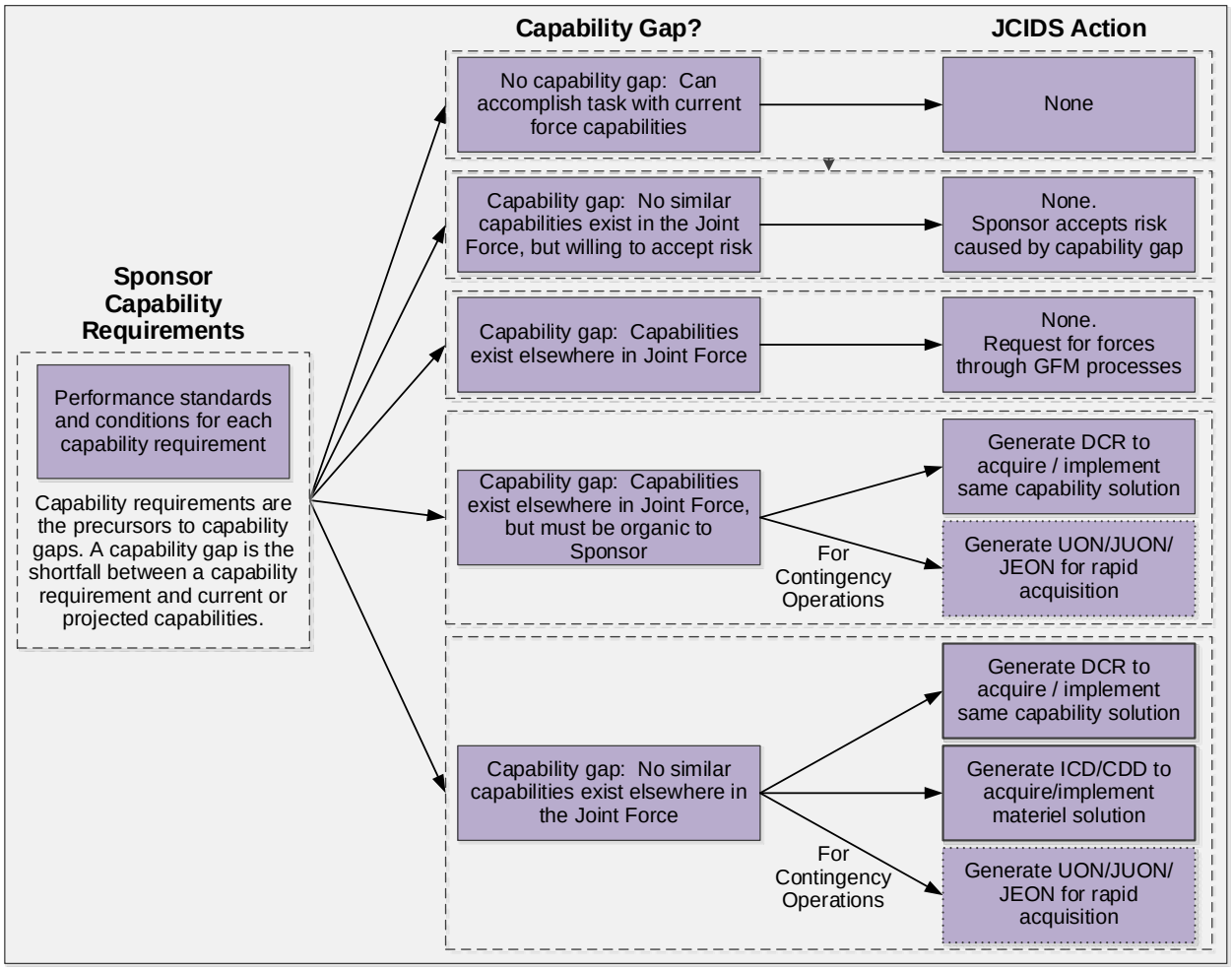

Figure C- 3: Identification of Capability Gaps and Resulting JCIDS Action

4.1. Issues not requiring JCIDS action. Not every capability gap will result in an associated JCIDS action, as each is a balance between operational risk of the capability gap, lifecycle costs associated with developing and sustaining a capability solution, and other factors.

4.1.1. New capability requirements documents are not appropriate if the Sponsor identifies capability solutions currently available to the joint force or in development. This also applies to cases where a Sponsor elects to move within the threshold and objective trade space of a validated capability requirements document.

4.1.2. If capability solutions which can satisfy the Sponsor capability requirements do not exist in the joint force, but the Sponsor is willing to accept risk, then no capability requirements document is generated.

4.1.3. If capability solutions which can satisfy the Sponsor capability requirements exist elsewhere in the joint force, the Sponsor does not create a new capability requirements document, but uses a Request for Forces (RFF) or Request for Capabilities (RFC) via the GFM process to request forces and their associated capabilities IAW References [142] and [148].

4.1.4. If the Sponsor identifies DOTmLPF-P capability solutions that can be implemented through a FPO and/or existing change process and do not rise to the level of JCB Interest.

4.2. Issues requiring JCIDS action. If the Sponsor identifies capability requirements which they cannot satisfy with capability solutions currently available to the joint force or in development, then they have a capability gap which may require further action.

4.2.1. If capability solutions which can satisfy the Sponsor capability requirements exist elsewhere in the joint force, but must be organic to the Sponsor organization:

4.2.1.1. To leverage entire capability solutions "off the shelf," the Sponsor may generate a Joint DCR for validation in JCIDS to establish the capability requirement for the fielded capability solution in the Sponsor organization. In urgent situations supporting ongoing or anticipated contingency operations, the Sponsor may generate a JUON, JEON, or DoD Component UON for greater expediency. Sponsors must articulate why the GFM process, and leveraging other capabilities of the joint force, is not appropriate to satisfying the Sponsor's capability requirement.

4.2.1.2. To leverage only portions of fielded capability solutions, to be integrated into one or more of the Sponsor's capability solutions, the Sponsor may generate a Joint DCR for validation in JCIDS to establish the requirement to leverage part of another Sponsor's capability solution. The implementation of the Joint DCR may involve updates to validated CDDs to provide for broadened scope, and submittal for review and revalidation.

4.2.2. If capability solutions which can satisfy the Sponsor capability requirements do not exist in the joint force, the Sponsor has three primary options:

4.2.2.1. If the capability requirement can be satisfied through a non-materiel approach:

4.2.2.1.1. For non-materiel solutions which impact only the Sponsor organization, review, validate, and implement IAW policies and processes of that organization.

4.2.2.1.2. For non-materiel solutions which impact more than just the Sponsor organization, generate a Joint DCR for validation in JCIDS, to establish a new non-materiel solution in the Sponsor organization. Joint DCRs may also be used in a similar manner to validate capability requirements where service contracting IAW Reference [149] provides the most appropriate capability solution.

4.2.2.2. Following the CBA, if the optimal approach to satisfying the capability requirement – a non-materiel approach, a materiel approach, or a combination of the two – the Sponsor may generate an ICD for validation in JCIDS. Sponsor analyses following ICD validation, such as an AoA, additional DOTmLPF-P

analysis, or other study, will determine which successor documents – Joint DCRs for non-materiel solutions and/or CDDs for materiel solutions – are to be generated and submitted to JCIDS to support follow-on efforts. For further information about the conduct of AoAs following ICD validation, see Reference [150]

4.2.2.3. If the capability requirements are driven by ongoing or anticipated contingency operations, and left unfulfilled would result in unacceptable loss of life or critical mission failure, the Sponsor may generate a JUON, JEON, or DoD Component UON document for expedited staffing and validation in the JCIDS or DoD Component processes. JUONs, JEONs, and DoD Component UONs are only generated when other means to satisfy the capability requirement are not practical – GFM process, JMVP, deliberate requirements and acquisition, etc. Warfighter issues, including the acquisition of materiel capability solutions in response to validated capability requirements, are addressed IAW Reference [26].

5. Documentation of Studies/Analysis and Associated Data.

5.1. Purpose. The Joint Staff Gatekeeper maintains a studies repository within the KM/DS system to facilitate visibility into, and potential reuse of, studies related to capability requirements and the generation of capability requirements documents. Organizations conducting studies will provide results of any studies or analyses intended to support capability requirements documents to the studies repository.

5.1.1. Posted study results facilitate more streamlined requirements documentation, allowing capability requirements documents to refer to the study data rather than replicate information unnecessarily. Historical study data in the repository also facilitates leverage of prior studies and efforts across the joint force to reduce unnecessary duplication of prior efforts and enable shorter timelines with more focused study efforts.

5.1.1.1. Sponsors will submit CBAs and other studies/data focused on identifying and assessing capability requirements to the studies repository before submitting an ICD based upon those efforts.

5.1.1.2. AoA study plans, AoA final reports, and other supporting documentation for the post-AoA (or similar study) review will also be archived in the studies repository ahead of the post-AoA (or similar study) review.

5.1.1.3. The studies repository is also used to capture assessments of JCTDs, fielded JUONs, JEONs, and DoD Component UONs, and other demonstrations of capability solutions in an operational environment, as well as other alternate forms of supporting documentation for capability requirements.

5.1.1.4. Study initiation notices for any related activities will be posted to the study repository at the start of the respective study.

5.1.2. To the greatest extent possible, the organizations conducting studies are to leverage historical information from the studies repository and other

sources, and focus CBAs and other studies only in areas which require new or updated analysis.

5.2. Submission of studies and associated data.

5.2.1. If details of a study, copy of an assessment, or other documentation intended to justify a capability requirement is not in the studies repository at the time the Sponsor intends to submit a related capability requirements document, the Sponsor will provide the supporting documentation before submitting the related capability requirements document for staffing and validation. Procedures for submission of studies and other data to the studies repository are outlined in Appendix C to Enclosure A of this manual.

5.2.2. Results of studies indicating that there is a lack of a need to pursue new capability requirements still are to be provided to the studies repository for future reference. This "negative" conclusion can prevent unnecessary duplication of studies reaching the same negative conclusion. Altered strategic guidance, threats, or other conditions in the future, may also allow the prior study to be used to support different conclusions in a much shorter timeframe, if available for review and modification.

5.3. Study initiation notices. Organizations conducting studies intended for or likely to drive submission of new capability requirements in the JCIDS process will provide a study initiation notice to the studies repository. This will help facilitate greater visibility into ongoing studies, encourage collaboration, and reduce unnecessary duplication of current study efforts.

5.3.1. For AoAs subject to CAPE approval of study guidance, such as for ACAT I programs, visibility into CAPE approval of AoA study guidance serves to inform JCIDS stakeholders that an AoA is underway.

5.3.2. For AoAs or similar studies not subject to CAPE approval of study guidance, such as for ACAT II or III programs, Sponsors will submit a study initiation notice to the studies repository.

5.3.3. Study initiation notices provided to the studies repository are to be concise but provide sufficient information for a reader to determine if the scope of the study is of interest and worth contacting the POC for further information or discussion. The notice is to be in memo format and contain at least the following elements:

5.3.3.1. Date of the notification memo.

5.3.3.2. Title of the study.

5.3.3.3. Executive summary/purpose of the study.

5.3.3.4. Participating organization(s).

5.3.3.5. Intended completion date.

5.3.3.6. Lead organization POC and contact information.

5.3.3.7. Tier 1 through 3 JCAs related to primary focus of study. For broadly scoped studies where identification of tier 3 JCAs is not applicable, identify the focus of the study to the lowest appropriate JCA tier.

5.3.4. The Joint Staff Gatekeeper will notify FCBs with potential interest in the study topic based upon their respective JCAs. FCB members and other interested stakeholders can review the study initiation notices to determine if there is any opportunity for collaboration on or leverage of study efforts. As appropriate, interested stakeholders may contact the organization conducting the study to discuss potential for collaboration and/or shared study efforts.

5.3.5. In the event of a study being discontinued prior to providing any significant results, the organization conducting the study will provide a termination notice in the studies repository. The notice is to be in memo format and contain at least the following elements:

5.3.5.1. Date of the termination notice memo.

5.3.5.2. Title of the study from the original initiation notice.

5.3.5.3. Date of the original initiation notice memo.

5.3.5.4. Purpose/reason for cancellation (i.e., funding limitations superseded by or consolidated into another study effort (provide Reference info), or overcome by external events such as updated strategic guidance, altered threats, etc.)

5.3.5.5. Lead organization POC and contact information.

ANNEX A TO APPENDIX B TO ENCLOSURE C
EXAMPLE OPERATIONAL ATTRIBUTES

1. Overview.

1.1. Purpose. This annex is intended to provide a set of example operational attributes as a common basis for definition of capabilities in each of the JCAs. They are applicable to describing capability requirements in the conduct of CBAs and other similar analyses, and in authoring of ICDs. These examples are not exhaustive but represent the general kinds of operational attributes which are to be considered in identification of operational capabilities needed to satisfy organizational roles, missions, and tasks.

1.1.1. As operational attributes generally do not provide value in isolation, they must be expressed in meaningful combinations which contribute to mission success using that capability.

1.1.2. They also are not to present operational attributes which are system specific and would be more appropriate for performance attributes (KPPs, KSAs, and APAs) articulated in CDDs.

1.2. Applicability. This annex applies to the Joint Staff, Services, CCMDs, and other Department of Defense (DoD) Agencies.

1.3. Proponent. The proponent for this appendix is J-8/JCD. For questions, contact J-8/JCD at (703) 695-2705.

2. JCA Examples.

2.1. Force Integration Attributes.

2.1.1. Generic Attributes. Accuracy, Adaptability, Comprehensiveness, Credibility, Integration, Timeliness.

2.1.2. Readiness Reporting Example (JCA 1.4.1 – Force Integration, Force Management, Readiness Reporting). Capability to evaluate the status of XXX assigned unit capabilities from authoritative data source, against XXX assigned mission with XXX seconds to within XXX percent accuracy.

2.1.2.1. Building Partnership Attributes.

2.1.2.1.1. Generic Attributes. Agility, Breadth, Depth, Effect, Flexibility, Persistence, Utility.

2.1.2.1.2. Influence Foreign Audiences Example (JCA 8.1.2 – Building Partnerships, Communicate, and Persuade Partner Audiences). Capability to deliver DoD information/message to XXX percentage of population of partner nation XXX within XXX time of the event with XXX confidence.

2.2. Battlespace Awareness Attributes.

2.2.1. Generic Attributes. Accuracy, Adaptability, Comprehensiveness, Credibility, Innovativeness, Integration, Interoperability, Persistence, Survivability, Timeliness.

2.2.2. Anti-Submarine Wide-area Search Example (JCA 2.2 – Battlespace Awareness, Collection, Multiple Tier 3 categories): Capability to search XXX area of the ocean's surface; within XXX distance from a carrier strike group; in XXX timeframe, with XXX probability of detection; with XXX sea-state, day/night, and weather conditions; for a submerged adversary target with detectability characteristics XXX.

2.3. Force Application Attributes.

2.3.1. Generic Attributes. Accuracy, Adaptability, Capacity, Flexibility, Mobility, Persistence, Scalability, Security, Survivability, Timeliness.

2.3.2. Penetrating Munition Example (JCA 3.2.1 – Force Application, Engagement, Kinetic Means). Capability to engage a stationary target (or target moving at speed XXX); under XXX day/night and weather conditions; through protective materiel/thickness XXX; delivering effect XXX to adversary personnel; within XXX distance of impact; with XXX probability.

2.4. Logistics Attributes.

2.4.1. Generic Attributes. Accountability, Agility, Attainability, Capacity, Economy, Effectiveness, Enduring, Expeditionary, Flexibility, Integrated, Networked, Persistence, Precision, Reliability, Responsiveness, Scalability, Simplicity, Survivability, Sustainability, Tailorability, Visibility, Velocity.

2.4.2. Tactical Cargo Transportation Example (JCA 4.1.2 – Logistics, Deployment, and Distribution, Sustain the Force): Capability to transport cargo in units up to XXX weight and XXX/XXX/XXX length/width/height; over XXX distance in XXX timeframe; with XXX terrain, day/night, and weather conditions.

2.5. Command and Control Attributes.

2.5.1. Generic Attributes. Accessibility, Assured, Agility, Completeness, Interoperability, Latency, Relevance, Reliable, Resilient, Security, Simplicity, Timeliness, Understanding.

2.5.2. Issue Emergency Action Message Example (JCA 5.5.2 – Command and Control, Direct, Task): Capability to compose messages in XXX format; transmit from authenticated originator(s) XXX to recipient(s) XXX; in time between transmission and receipt no greater than XXX; with no greater than XXX probability of interception; with at least XXX probability of correct message receipt.

2.6. Communications and Computers Attributes.

2.6.1. Generic Attributes. Accessibility, Accuracy, Agility, Availability, Capacity, Completeness, Controllability, Expeditionary, Flexibility, Integration,

Interoperability, Latency, Maintainability, Configurability, Relevance, Reliability, Responsiveness, Robustness, Scalability, Security, Survivability, Throughput, Timeliness, Visibility.

2.6.2. Positioning, Navigation, and Timing (PNT) Example (JCA 6.2.4 – Communications and Computers, Enterprise Services, PNT). Capability to provide globally available PNT services, with horizontal and vertical accuracy of XXX and XXX meters, under background noise/jamming conditions XXX, with operational availability of XXX.

2.7. Protection Attributes.

2.7.1. Generic Attributes. Capacity, Effectiveness, Integration, Networkability, Persistence, Responsiveness, Survivability, Speed, Maneuverability, Detectability, Vulnerability, Durability, Resiliency, Recoverability.

2.7.2. Tactical Missile Defense Example (JCA 7.1.1 – Protection, Prevent, Prevent Kinetic Attack). Capability to defend a land or water surface area of XXX within XXX distance of a point defense location; against adversary ballistic and cruise missile threats with detectability characteristics of XXX and operating up to speeds of XXX; with threats operating singly or in salvos of up to XXX, with a probability of successful defense of XXX.

2.8. Corporate Management and Support Attributes.

2.8.1. Generic Attributes. Accessibility, Accuracy, Auditability, Availability, Efficiency, Integration, Interoperability, Latency, Reliability, Responsiveness, Security, Throughput, Timeliness, Usability, Visibility.

2.8.2. Financial Management Example (JCA 9.5.2 – Corporate Management and Support, Program Budget and Finance, Accounting and Finance). Capability to process XXX requests for payment within XXX timeframe, with payment error rate no greater than XXX, with real-time visibility to organizations XXX with latency no greater than XXX.

ANNEX B TO APPENDIX B TO ENCLOSURE C
CAPABILITY BASED ASSESSMENT GUIDE

1. Overview.

1.1. Purpose. A CBA provides a robust assessment of a mission area, or similar bounded set of activities, to assess the capability and capacity of the joint force to successfully complete the mission or activities.

1.1.1. A CBA often leads to the identification of new or modified capability requirements and associated capability gaps. If the capability gaps represent significant operational risk to the joint force, then these capability requirements, along with recommendations for materiel and/or non-materiel approaches for closing or mitigating the capability gaps, may be submitted for staffing and validation by the appropriate validation authority.

1.1.2. The intent of a CBA may also be satisfied through one or more other studies or analyses, as long as the analytical rigor and breadth of analysis is covered by the collective analytical efforts.

1.1.3. The information in this annex is meant to supplement the material presented in Reference [139]. Sponsors should make themselves familiar with this reference when conducting a CBA.

1.2. Applicability. This appendix applies to the Joint Staff, Services, CCMDs, and other DoD Agencies.

1.3. Proponent. The proponent for this annex is J-8/JCD. For questions, contact J-8/JCD at (703) 695-2705.

2. Capability Based Assessments.

2.1. Traceability. The analytical work conducted as part of a CBA provides the traceability between strategic guidance, operational missions, Service and Joint Concepts, CONOPS, DIA- or Service-approved threat products, including but not limited to, capability requirements, and capability solutions.

2.1.1. CBA activities support the development of required content in capability requirements documents and associated DoDAF products, as well as development of materiel and non-materiel capability solutions. These results are expected to be further refined throughout the follow-on processes.

2.1.2. A number of DoDAF views are to be used to capture results of a CBA, facilitating reuse in capability requirements documents, acquisition activities, and capability requirements portfolio management. For more details on applicable DoDAF views, see the DoDAF Primer in Appendix H to Enclosure B of this manual and Reference [6].

2.1.3. When one or more studies or analyses are used in place of a CBA, the Sponsor may need to consolidate the data from those studies into a single set of DoDAF products appropriate for the scope of the ICD.

2.2. Level of Rigor. The Sponsor must determine the level of analytic rigor needed in a CBA. The rigor used in a CBA is a function of the complexity of the mission being assessed, the consequences of operational failure, and the uncertainties of the Support for Strategic Analysis (SSA) products and other supporting data considered.

2.2.1. When performing a CBA relative to a validated capability solution that may require replacement, recapitalization, or evolution to meet future capability requirements, the Sponsor is starting from a known baseline and making excursions to address potential future capability requirements. In this case a CBA should take no more than 60-90 calendar days to demonstrate that replacement, recapitalization, or evolution is required. While the decision to consider recapitalization of an existing capability solution may be driven by a capability gap or set of gaps, a CBA must also consider the entire set of tasks, conditions, and standards fulfilled by the capability solution.

2.2.2. When performing a CBA that addresses capability requirements most likely addressed through an IS solution, the CBA should take no more than 90 calendar days. The determination on whether a new IS will be required or if a fielded system can be evolved to meet the need will be further considered in the AoA or similar study.

2.2.3. When performing a CBA that is examining a new mission with a lot of uncertainty or complexity or is assessing the capability requirements for a new Service and Joint Concept, the risks and uncertainty drive the need for a more comprehensive CBA to determine if it is necessary to move to an evolution of a fielded capability solution or to pursue transformational capabilities to satisfy the capability requirements.

2.2.4. One CBA may address any of these alternatives. In any case, the maximum time allotted for a CBA should be no more than 180 calendar days, and the assessment should be tailored to meet this objective. The time allotted does not include the required time needed for staffing and approval by the Sponsor.

2.3. Additional guidance. While this annex provides an overview of the CBA process, References [139] and service documents offer more detailed guidance and best practices relating to these assessments. Organizing and executing a successful CBA and satisfying the demands of strategic guidance is a significant challenge. Consequently, a CBA addressing a broad mission area must be conducted with a robust joint team that can bring the necessary breadth of expertise to bear on the problem.

3. CBA Process Steps.

3.1. Study Initiation Notice. Each CBA begins with the Sponsor providing a study initiation notice to the Joint Staff Gatekeeper. This provides visibility, and facilitates participation by other stakeholders who may have valuable input to contribute to a CBA, or may be able to leverage the output of the CBA for other ongoing activities.

3.1.1. The Sponsor must identify and build upon previous CBAs, studies, joint lessons learned, and other analytical products applicable to the area of interest. The intent is to avoid any unnecessary repetition of prior efforts, and provide continuity between analyses for reviewers and decision makers.

3.1.1.1. This does not preclude the CBA sponsoring organization from applying different context or different assumptions to previous analyses, as appropriate for the current CBA.

3.2. CBA Focus. The CBA's focus is derived from the strategic context, mission and scenarios to be examined, the timeframe under consideration, and the associated threats.

3.2.1. Strategic context. The CBA must be relevant to the needs of the defense strategy and other strategic guidance contained in documents such as the NDS, NMS, DPG, and GEF. The products generated by the JSCP in Reference [130] provide other data important for describing the breadth of the strategic environment and selecting an adequate scenario sample.

3.2.2. Missions and scenarios. The CBA must use appropriate OPLANs or CONPLANs for near-term assessments or SSA products developed IAW References [151] and [152] for long-term assessments. Furthermore, the SSA products must be chosen in such a way that the full spectrum of operational situations relevant to the defense strategy will be examined, including other U.S. Government agency/department, allied/partner nation, and coalition activities. While it is important to scope the assessment to make it manageable, it is equally important to cover the spectrum of strategically relevant operational situations.

3.2.3. Joint Lessons Learned. The CBA also needs to be informed by the Joint Lessons Learned Information System (JLLIS), IAW References [138] and [146], to provide additional information relevant to the CBA area of interest. JLLIS is the DoD system of record and enterprise solution supporting the Chairman's Joint Lessons Learned Program.

3.2.4. Use of DoDAF views.

3.2.4.1. DoDAF views and associated data provide a structured means to document data associated with the CBA and more easily leverage and update data when developing capability requirements documents as shown in Figure C-4.

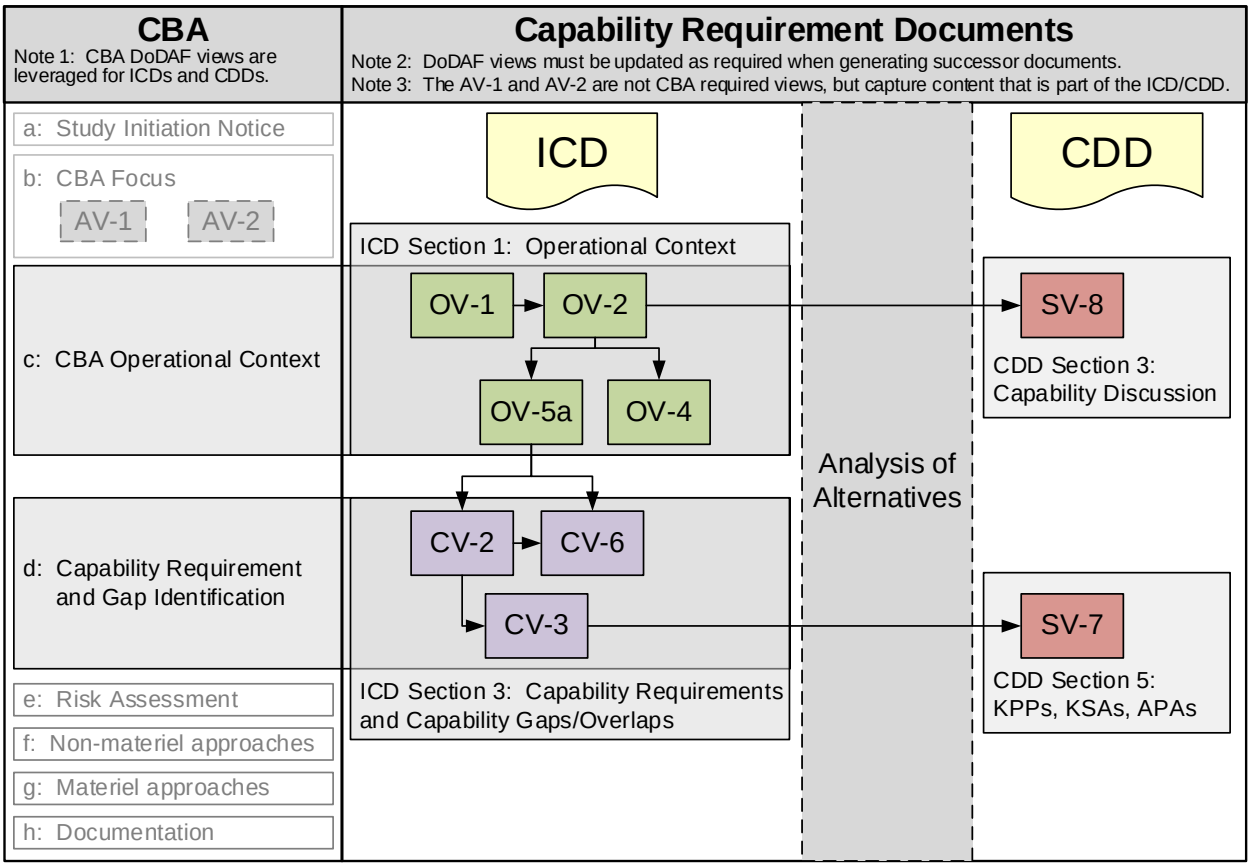

Figure C- 4: DoDAF Flow from CBA to Capability Requirements Documents

3.2.4.2. DoDAF views and associated data are intended to represent the context under which the CBA was conducted (i.e., the existing enterprise) as modified, if applicable, by the recommendations of the CBA (i.e., the proposed future end state). Aspects of the existing Enterprise Architectures not impacted by the CBA recommendations must remain unchanged.

3.2.4.3. The DoDAF OVs and CVs illustrated in Figure C-4 are to be generated during the CBA, as leveraging these DoDAF views and associated data can significantly improve efficiency, saving time and resources later in the JCIDS and DAS processes.

3.2.4.3.1. Note that the level of detail in DoDAF views generated during a CBA does not require the use of sophisticated architecture tools and associated personnel unless desired by the Sponsor. The required data for most of the views can be structured as tables using Microsoft Excel or similar spreadsheet programs and used in that form for the purposes of generating capability requirements documents and submitting associated DoDAF views for review. The data must be submitted in such a form that it may be efficiently imported into architecture tools for follow-on efforts as desired by the Sponsor and other stakeholders. Providing only image files, Microsoft PowerPoint briefings, or other non-importable formats is not acceptable, as all data would need to be

regenerated in an importable format prior to further use. Examples of DoDAF views supporting JCIDS are available at the URL in Reference [3].

3.2.4.3.2. Data captured in the DoDAF views during the CBA may be limited by knowledge at that stage of development but will be updated throughout follow-on stages of JCIDS and DAS as more detail is gained.

3.2.4.4. The DoDAF SVs illustrated in Figure C-4 are NOT to be generated during the CBA and are shown for context only. SVs can be developed during the Materiel Solutions Phase as recommended by the ICD, and therefore may be available before AoA, though some system level details may not be available until after an AoA is conducted.

3.2.4.5. In addition to views outlined in later sections of the CBA guidance, the Sponsor may elect to maintain/update the following views throughout the CBA activities for their own benefit, even though they are not mandatory submissions to go along with an ICD.

3.2.4.5.1. DoDAF AV-1 – Overview and Summary Information. This overview/summary data from the CBA can be re-used when authoring the CBA results and the ICD executive summary

3.2.4.5.2. DoDAF AV-2 – Integrated Dictionary. The definitions identified during the CBA can be re-used when authoring the CBA results and as a starting point for authoring the ICD Appendices B and C.

3.3. Operational Context. The next step in the CBA is to consider the timeframe under consideration, applicable threats, and relevant Service and Joint Concepts, CONOPS, objectives, and related effects to be achieved.

3.3.1. Timeframe. The timeframe considered in the CBA is important both to help establish the conditions and threats under which the mission is to be carried out, and as a key component in discussions between the requirement Sponsor and the acquisition community in determining the required IOC and FOC dates. The IOC and FOC dates indicate when the joint warfighter needs initial and full capability provided by one or more capability solutions. The timing of IOC and FOC from this CBA step, together with the required capabilities identified in a later CBA step, supports development of the DoDAF CV-3 later in the CBA when phasing of capability requirements is considered, and supports re-use when authoring the ICD operational context section. This view is important when the operational context envisions the requirement for some of the identified capabilities to be available at earlier dates than other identified capabilities.

3.3.2. Threats. Threats to the mission being analyzed must be derived from DIA- or Service-approved threat products, including but not limited to product using relevant Threat Modules, the MSFD, and the Joint Country Forces Assessments. If additional assistance is required, contact DIA's Defense Technology and Long-Range Analysis (DIA/TLA) office, Acquisition Threat Support Division via the options shown in Reference [153]. DIA/TLA support

to JCIDS includes data provided by multiple types of DIA- and Service-validated threat products.

3.3.2.1. Collaboration among the intelligence, counterintelligence (CI), requirements, and acquisition communities shall be maintained throughout the capability solution's lifecycle to achieve the highest level of technological superiority possible over adversarial capabilities. This collaborative effort includes identification of adversary threat capabilities that represent the projected operational environment, and the anticipated capabilities and CONOPS that adversaries might employ against the capability being reviewed. These collaborative assessments are used as inputs to the Sponsor's studies, analyses, and other efforts in requirement development efforts.

3.3.2.2. Operational tasks, conditions, and standards identified in studies or other analyses are to be submitted to DIA/TLA to enable production of an initial threat environment assessment VOLT report. The VOLT report identifies projected adversarial threat capabilities which are a factor in setting the capability requirements and initial objective values, including scientific and technological developments which could specifically affect the determination of capability requirements and development of capability solutions. DIA/TLA, and the Defense Intelligence Threat Library (DITL) will continue to assist Sponsors, as needed, with updates to the threat assessments throughout the remainder of the capability solution's lifecycle until superseded by a DIA- or Service-approved threat product including but not limited to, the DITL and the VOLT.

3.3.2.3. Characteristics of adversary threat capabilities which are a factor in establishing capability requirements and associated initial objective values are to be documented as proposed CIPs. In cases where CIPs are already identified in existing DIA- or Service-approved threat products, identify which approved CIPs are associated with threat-dependent capability requirements identified in the CBA. If there are no approved CIPs that apply to the threat-dependent capability requirements identified in the CBA, draft proposed CIPs that can be included in the ICD and reviewed and approved as part of the threat certification activities. This enables the IC to provide more robust monitoring of threat changes throughout a capability solution's lifecycle.

3.3.3. Concepts and CONOPS. Concepts and CONOPS used as part of a CBA must be documented such that the reviewers and validation authorities can understand the context used to identify the capability requirements.

3.3.3.1. Joint concepts, developed IAW Reference [131], describe how a Joint Force Commander might employ new capabilities to meet future challenges and are to be used as a starting point where applicable.

3.3.3.2. Concepts and CONOPS must clearly identify whether operations are required in, or after exposure to, Chemical, Biological, Radiological, or Nuclear (CBRN) environments, through degraded GPS or cyber situations, or under the effect of other potential adversary stressors.

3.3.3.3. There is no strict format for a concept or CONOPS used in a CBA, but it must describe the following areas at a minimum:

3.3.3.3.1. Problem being addressed.

3.3.3.3.2. Mission expected to be performed.

3.3.3.3.3. Commander's intent.

3.3.3.3.4. Operational overview over the full range of military operations.

3.3.3.3.5. Objectives to be achieved.

3.3.3.3.6. Roles and responsibilities of tasked organizations.

3.3.3.4. The level of detail provided with the concept or CONOPS provides the required data needed for the Sponsor to generate the following DoDAF views, if DoDAF views are not already provided as part of the concept or CONOPS. Each view serves as a starting point for further refinement and exploration of alternative concepts or CONOPS during the CBA.

3.3.3.4.1. DoDAF Operational View (OV)-1 – High Level Operational Concept Graphic. The OV-1 provides stakeholders with a graphical view of the highest level of the concept or CONOPS to facilitate general understanding of the concept or CONOPS. The OV-1, as refined during the CBA, is reused in the capability requirements documents and other follow-on efforts.

3.3.3.4.2. DoDAF OV-2 – Operational Resource Flow Description. The OV-2 translates the OV-1 picture into a complete set of nodes, activities, and interconnections upon which the rest of the architecture is based. This view must focus on the operational activities/effects necessary to execute the concept or CONOPS and avoid the appearance of having made "pre-determined" capability solutions which will be explored in a later step of the CBA. This provides stakeholders with more detailed operational interactions which must take place between nodes/actors executing the concept or CONOPS, and any enabling/supporting capabilities which are involved, including identification of organizations that may be involved. The OV-2, as refined during the CBA, provides the fundamental basis for traceability from other DoDAF views and content in capability requirements documents back to the operational activities/effects applicable to the concepts and CONOPS.

3.3.3.4.3. DoDAF OV-4 – Organizational Relationships Chart. The OV-4 provides stakeholders with an initial overview of the organizations intended to satisfy the concepts and CONOPS. This provides a baseline for excursions during and following the AoA (or similar study), as greater detail of potential capability solutions and associated organizations is developed.

3.3.3.5. Any CONOPS used as the basis for a CBA must be approved by the CBA sponsoring Component at a minimum.

3.3.3.5.1. Approved Service and Joint Concepts or CONOPS, coupled with the SSA products, are to be further refined to describe how the objectives are

achieved with current or programmed forces, using doctrinal approaches. These refinements include a logical projection of how current concepts and CONOPS might be expected to evolve for the timeframe under consideration.

3.3.3.5.2. Alternative Service and Joint Concepts, or alternative CONOPS, based on non-doctrinal approaches or changing the original approved concepts, also may be considered to close or mitigate the capability gap by using fielded capability solutions in a different manner.

3.3.4. Identification of operational tasks.

3.3.4.1. The military objectives outlined in the OPLANs, CONPLANs, and SSA products, including mission outcomes and associated desired effect, provide a source for developing the list of required tasks.

3.3.4.2. The applicable concepts and CONOPS, and variations considered within the CBA provide the framework for developing lists of required tasks needed to accomplish both the proposed and alternative CONOPS. The UJTL outlined in Reference [154] also provides a framework to aid in identifying and organizing the tasks, conditions, and required capabilities. If the UJTL does not identify appropriate tasks for the Service and Joint Concepts or CONOPS under consideration, submit updates to the UJTL IAW Reference [154], using the tools available at the URL in Reference [8].

3.3.4.3. While performing a CBA, do not lose sight of cross-cutting functions, such as logistics, communications, and intelligence, which may have different dependencies when considering different concepts or CONOPS for addressing the capability requirements. The energy supportability analysis, described in Annex E to Appendix G to Enclosure B of this manual, and intelligence supportability analysis, described in Annex G to Appendix G to Enclosure B of this manual, provide additional guidance on conducting the appropriate analysis.

3.3.4.4. DoDAF OV-5a – Operational Activity Decomposition Tree. The Sponsor captures the output of this step in the OV-5a, which provides the relationship between the operational activities/effects from the OV-2 and the associated UJTs. The OV-5a, as refined during the CBA, provides traceability from other DoDAF views and content in capability requirements documents back to the UJTs applicable to the concepts and CONOPS.

3.3.5. Level of detail. The analysis of required concepts and CONOPS needed for this section of the CBA provides the Sponsor with a robust understanding of the operational context and tasks which must be performed and supports further refinement and exploration of excursions during the CBA.

3.3.5.1. At the early stage of a CBA, only the “as-is” architecture of developed capabilities will be available in great detail. The DoDAF views related to the proposed capabilities will be captured in much less detail at this stage but must be consistent with the concept(s) or CONOPS.

3.3.5.2. System specific details are to be avoided at this stage so that the later AoA or similar studies can be conducted with maximum flexibility, and allow DoDAF views to mature as additional decisions are made and data is generated throughout the JCIDS and DAS processes.

3.4. Capability Requirement and Capability Gap Identification.

3.4.1. The CBA Sponsor must identify the capability requirements which enable the activities/effects and UJTs identified in the DoDAF OV-2 and OV-5a views, and through an assessment of current and programmed forces, identify any associated capability gaps and potential force redundancies for each scenario. Note that while some redundancies are intentional for the purpose of providing resiliency, unnecessary redundancies should be minimized.

3.4.1.1. The operational conditions are derived from SSA products, and capability requirements are derived from tasks that must be accomplished to achieve the objectives under those operational conditions. The capability requirements and capability gaps must be described in terms of the SSA products assessed and the impact on achieving the relevant objectives. It is likely that the capability gaps will be inconsistent across different SSA products, so it is essential to associate identified capability gaps to their operational context.

3.4.1.2. For capabilities provided by IS, the CBA should use a DoD enterprise architecture as explained in Reference [64]. To describe and characterize system contributions to military operations, use the DoD Data Framework and the Joint Command and Control (C2) Reference architecture for SECRET and below systems, and the Defense Intelligence Information Environment (DI2E) data construct for intelligence systems IAW References [6], [155], and [156].

3.4.2. The CBA must explain the methodology for determining the capability requirements and associated capability gaps, to ensure that the association between the capability requirements and strategic guidance is clear. A framing construct, such as the CML presented in Figure C-2, must be used to provide rigor to the traceability from strategic guidance, operational missions/scenarios, and threats, to the decomposition into capability requirements and conditions associated with UJTs. The framework used must also provide context for the comparison of capability requirements to the fielded and programmed capability solutions of the joint force as a means to identify operational risks associated with any capability gaps.

3.4.2.1. The JCA framework outlined in Reference [56] is a logical grouping of capabilities that provides the structure that capability requirements and associated capability gaps can be aligned with the Department's capability requirements portfolios to correlate similar needs, leverage common capability solutions, and synchronize related activities. The Sponsor is required to identify capability requirements to the Tier 3 JCAs, but lower levels are recommended to provide additional clarity to the capability requirements.

3.4.2.2. DoDAF Capability View (CV)-2 – Capability Taxonomy. As the Sponsor identifies capability requirements and associated capability gaps, they can generate the CV-2 and specify the taxonomy associated with these capabilities. These capability requirements are to be captured in a manner consistent with the operational attributes outlined in Annex A of Appendix B of this enclosure, and be expressed in terms of operational effectiveness rather than performance of a presumed capability solution. Quantitative criteria for mission success must be established for each capability requirement to support later assessment of how well potential materiel solutions satisfy the capability requirements. In most cases, these criteria will not be simple pass-fail standards, but instead will represent a continuum of values.

3.4.2.3. DoDAF CV-3 – Capability Phasing. The Sponsor builds upon the CV-2 with any applicable phasing of the identified capability requirements and captures that in the CV-3. For example, if only a subset are needed in a shorter timeframe than the required timeframe for the entire set of capabilities, the CV-3 captures the required information to pursue an incremental development strategy while making sure that the correct capabilities are introduced at the correct times.

3.4.2.4. DoDAF CV-6 – Capability to Operational Activity Mapping. The Sponsor uses the CV-6 to ensure robust traceability between the identified capability requirements in the CV-2 and the identified operational activities in the OV-5a. This reduces the risk of disconnects between delivered capabilities and the operational activities they are intended to satisfy.

3.4.3. Once the capability requirements are identified in the steps above, any shortcomings in the current or programmed force can be identified as capability gaps. The capability gaps can be characterized as:

3.4.3.1. Lack of proficiency (inability to achieve the relevant effect in certain conditions).

3.4.3.2. Lack of sufficiency (inability to bring capable forces to bear due to force shortages or other commitments).

3.4.3.3. Lack of any fielded capability solution.

3.4.3.4. Lack of interoperability/integration (required capabilities exist piecemeal and are not capable of interacting to create desired effect).

3.4.3.5. Need for replacement due to aging (fatigue life, technological obsolescence, etc.) of a fielded capability solution.

3.4.3.6. Policy limitations (inability to use the force as needed due to restrictions in effect).

3.5. Risk Assessment.

3.5.1. The capability gaps are then assessed against adversary threats in terms of the risk to mission (the ability to achieve operational objectives), the risk to force (the potential losses due to the gap), and other key considerations,

such as resourcing risks and effects on allies, partner nations, and other U.S. Government agencies/departments. The conditions and standards developed for the associated tasks provide the basis for the assessments. JP 2-01.3, Joint Intelligence Preparation of the Operational Environment, provides additional guidance on threat assessment and risk analysis that the joint warfighter will need to be familiar with.

3.5.2. Since a validation authority for capability requirements documents will ultimately decide which capability gaps are important enough to develop new capability solutions, the capability gaps must be directly associated to operational situations and risk to operational objectives. Figure C-5 presents an example approach for assessing the risks and consequences associated with a capability gap. The capability gap is assessed based Component functions and their impact on several areas: Ability to achieve the objectives; operational timelines; resources; unanticipated requirements; force provider resourcing; force management and institutional capacity.

Risk	Criteria	Low	Moderate	Significant	High
CCMD "Risk to Mission" Ability to execute assigned missions at acceptable human, materiel, financial, and strategic cost.	Achieve Objectives (CCMD Current Operations)	Very Likely (81-100%) Can achieve all objectives	Likely (51-80%) Can achieve all critical objectives	Unlikely (21-50%) Can achieve only most critical objectives	Highly Unlikely (0-20%) Potential failure; can't achieve critical objectives
	Achieve Plan Objectives (Contingencies)	As Planned (Minimal Costs)	Limited Delays (Acceptable Costs)	Extended Delays (Substantial Costs)	Extreme Delays (Unacceptable Costs)
	Authorities	Full authority provided to achieve all objectives	Sufficient authority only provided to achieve most objectives; no critical shortfalls	Insufficient authority provided to achieve some critical objectives	Insufficient authority for key objectives; potential mission failure
	Resources Needed to Meet Required Timelines	As Planned (Minimal Costs)	Limited Delays (Acceptable Costs)	Extended Delays (Substantial Costs)	Extreme Delays (Unacceptable Costs)
Service/JFP "Risk to Force" Ability to generate trained and ready forces, and to plan for, enable, and improve national defense.	Meet CCDR Requirements (CCMD Current Operations)	GFM Sourced ≥ 90% (Some Shortfalls)	GFM Sourced ≥ 80% (No Critical Shortfalls)	GFM Sourced ≥ 70% (Critical Shortfalls)	GFM Sourced ≥ 90% (Shortfalls Cause Mission Failure))
	Meet CCDR Requirements (Contingencies)	Full capacity to source all requirements	Shortfalls cause minor plan deviations	Shortfalls cause major plan deviations	Shortfalls cause plan failure
	DOTmLPF-P Capability vs. Threat	Dominance	Superiority	Parity	Inferiority
	Readiness	Full Spectrum C1 Full Capacity	Ready for MCO C1/C2 Some Capacity Shortfalls	Ready for Minor Armed Conflict Critical Capabilities C1/C2	Critical Capabilities ≤ C2 Capacity Shortfalls Cause Mission Failure
	Stress on the Force (Active Component)	Limited Stress (DT > 1:2)	Moderate Stress (1:2 > DT > 1:1.5)	Major Stress (1:1.5 > DT > 1:1)	Extreme Stress (DT < 1:1)
	Stress on the Force (Reserve Component)	Limited Stress (DT > 1:5)	Moderate Stress (1:5 > DT > 1:4)	Major Stress (1:4 > DT > 1:3)	Extreme Stress (DT < 1:3)
	Programmatic	Meets or exceeds schedule, IOC or FOC; incurred savings	Minor delays, milestone ≥ B Minor budget difficulty	Major delays, milestone ≤ A Over Budget (Nunn-McCurdy)	Program failure, Zeroed Out (De-funded)

Risk	Criteria	Low	Moderate	Significant	High
	Force Development & Industrial Base	Meet all mission requirements	Meet priority mission requirements (no critical shortfalls)	Critical shortfalls cause major plan deviations	Failure to meet essential requirements causes mission failure

Figure C- 5: Example Approach for Assessing Risks

3.5.3. While capturing risk levels is one aspect of the assessment, it is more critical to identify what tasks cannot be completed or what operational impacts will be in effect if a capability gap goes unmitigated.

3.6. Non-materiel approaches. If the CBA identified capability gaps with an unacceptable level of operational risk, the Sponsor then determines if a non-materiel approach can close or mitigate any of the capability gaps by recommending changes to one or more of the DOTmLPF-P areas:

3.6.1. Joint Concepts, Service Concepts and CONOPS, using non-doctrinal approaches. The baseline assessment should only consider doctrinal CONOPS, but the non-materiel approach assessment may consider non-doctrinal alternatives, particularly those documented in approved Service or Joint Concepts. Where applicable, alternatives must also consider CONOPS involving allied/partner nation or other U.S. Government agency/department participation.

3.6.2. Organizational and personnel alternatives. A CBA cannot redesign the force, but it can suggest how certain functions can be strengthened to eliminate gaps and identify mismatches between force availability and force needs. Finally, note that operating the programmed force under substantially different organizational or personnel assumptions will generally require the development of an alternative CONOPS to support those assumptions.

3.6.3. Training alternatives. The CBA is to consider if changes to training could improve effectiveness of existing capabilities or allow the introduction of new capabilities using existing materiel.

3.6.4. Alternative uses of fielded materiel. The CBA is to consider how existing materiel within an organization might be used in a new or unconventional manner to close or mitigate capability gaps and reduce operational risk. The CBA should also consider the use of materiel fielded to other DoD Components, other U.S. Government agencies/departments, allied/partner nations, coalition partners, etc.

3.6.5. Leadership and Education alternatives: The CBA is to consider if changes to leadership and education could improve effectiveness of existing capabilities, or introduce new capabilities using existing materiel.

3.6.6. Facility alternatives. The CBA is to consider how existing facilities within an organization might be used in a new or unconventional manner to close or mitigate identified capability gaps, and reduce operational risk. The CBA should also consider the use of facilities not currently available within the organization, but fielded to other DoD Components, other U.S. Government

agencies/departments, allied/partner nations, coalition partners, etc. The CBA may also consider how new facilities and/or locations may help to close or mitigate identified capability gaps, and reduce operational risk.

3.6.7. Policy Alternatives. When considering policy alternatives, the CBA must document which policies are contributing to capability gaps and under which circumstances. A policy change that allows new applications of fielded capabilities or modifies force posture to increase deterrence is always of interest and should be considered. Policy alternatives should identify changes to support engagements with non-DoD forces – other U.S. Government agency/department, allied/partner nation, coalition – required to address the related Service and Joint Concepts, CONOPS, and SSA products.

3.7. Materiel approaches. If unacceptable risk remains after considering the application of non-materiel approaches, the Sponsor then assesses general approaches for materiel capability solutions which can eliminate or mitigate the capability gaps. Three categories of materiel approaches are:

3.7.1. Evolution of fielded capability solution(s) with significant capability improvement, including development and fielding of improved IS, improved components or subsystems to address high obsolescence rates, or other upgrades and product improvements.

3.7.2. Replacement or recapitalization of a fielded capability solution(s) with significant capability improvement. The CBA is to also consider impact on retirement of fielded capability solution(s) as the new capability solution is brought into service, and whether overall quantities in the joint force should be reduced based on increases in capability.

3.7.3. Introduction of a transformational capability solution(s) that differ significantly in form, function, operation, and capabilities from fielded capability solution(s). They may address capability gaps associated with a new mission or describe breakout capabilities that offer significant improvement over current capability solutions or transform the ways of accomplishing a mission.

3.7.4. Increase integration/interoperability of existing Service capabilities to create new SoS.

3.8. CBA Documentation.

3.8.1. Upon completion, the Sponsor provides results of the CBA, or other studies intended to identify capability requirements and associated capability gaps, to the Joint Staff Gatekeeper for visibility and to support review of subsequent capability requirements documents. As CBAs serve as a means for Sponsors to identify their capability requirements and associated capability gaps, they are not validated through the JCIDS Process. Conduct of the CBA and approval of the results are at the discretion of the Sponsor.

3.8.2. Following completion of the CBA, the Sponsor may offer recommendations for the most appropriate approach(es) to close or mitigate

capability gaps and reduce operational risk by generating and submitting one or more capability requirements documents for review and validation by the appropriate validation authority.

(INTENTIONALLY BLANK)

ENCLOSURE D

REQUIREMENTS MANAGEMENT CERTIFICATION TRAINING

1. Overview.

1.1. Purpose. The purpose of this enclosure is to provide an overview of the requirements management certification process.

1.2. Applicability. IAW Reference [157], members of the Armed Forces and employees of DoD with responsibility for generating capability requirements must successfully complete requirements certification training. The Defense Acquisition University (DAU) has the responsibility for providing the congressionally mandated baseline training.

1.2.1. DAU, in consultation with Joint Staff and OUSD(A&S), developed a training program for DoD personnel with responsibility for developing requirements. DoD Components identified the target population for the training program.

1.2.2. As personnel have varying degrees of responsibility within the requirements process, and correspondingly variable training needs, each DoD Component (Joint Staff, Military Service, Combatant Command, or Defense Agency) determines what steps are required to certify their personnel as Requirements Managers. Completion of the appropriate DAU certification course(s) described herein provides the common baseline and must be accomplished prior to certification. DoD Components can mandate additional requirements courses and/or training to meet individual Component needs.

1.2.3. DoD Components, and their Gatekeeper personnel, are ultimately responsible for ensuring that capability requirements documents are in compliance with guidance in References [1] and this manual.

1.3. Proponent. The proponent for this enclosure is the Center Director, Requirements Management, Defense Systems Management College (DSMC), DAU. For questions, contact DAU at (703) 805-2381.

2. Requirements Management Certification Training (RMCT).

2.1. Certification levels. Individuals filling positions/billets within a DoD Component whose responsibilities are commensurate with the guidelines below will be trained to the level associated with those responsibilities.

2.1.1. Level A – *Requirements Apprentice* – Support activities focused on requirements generation and capability development, including but not limited to: assist in defining user needs, assist with related studies and reports, provide subject matter expertise, assist in document drafting and staffing.

No significant requirements experience or DAU prerequisites are required for typical Level A positions/billets. Examples of job related tasks at this level may include: participate in Integrated Product Teams (IPT) developing capability

requirements; assist with drafting, coordination and staffing of JCIDS documents, associated materials and media; support Capability Based Analysis (CBA) teams; support Analysis of Alternatives team; attend service or acquisition led program reviews; fundamental working knowledge of service policies and procedures for requirements related issues.

2.1.2. Level B – *Requirements Journeyman* – Engage in activities focused on requirements generation and capability development, including but not limited to: draft capability requirements documents, participate in requirements related IPTs, participate in requirements related studies and analysis, facilitate document development across organizations.

Level B billets/positions are typified as those requiring familiarity with terminology, policies and procedures associated with requirements generation, plus equivalent familiarity with acquisition and resourcing as they relate to requirements. Those filling Level B billets/positions may work directly with program office and resource office personnel. Examples of job related tasks at this level may include: lead requirements related IPTs; participate as member of acquisition program IPTs; significant role in CBA or similar efforts; contribute as SME in AoA or similar efforts; coordinate requirements issues with program offices; coordinate requirements documents among service-level stakeholders; coordinate presentations to service, joint and/or OSD requirements review panels; assist in the development of DoDAF Architecture Products.

2.1.3. Level C – *Requirements Core Expert* – Lead or coordinate activities focused on requirements generation and capability development, including but not limited to: writing and editing capability requirements documents, participate in requirements related IPTs, significant role in requirements related studies and analysis.

Personnel filling Level C billets/positions must have Level B training, and are typified as experienced with the terminology, policies and procedures associated with requirements, acquisition and resourcing. Examples of job related tasks at this level may include: lead or coordinate development of CONOPS or similar documents; represent service, agency for CCMD in requirements, acquisition and resourcing forums; support presentations at service capability requirements councils/boards; lead, coordinate or support presentations at joint staff forums (including working group, FCB, JCB and JROC forums); finalize JCIDS documents for service-level approval; adjudicate staffing comments on capability documents; lead or coordinate development of DoDAF Architecture Products; assist service-level action officers with resource justification material; provide input to cost and affordability venues as related to requirements issues.

2.1.4. Level D – *Requirements Validators and Prioritizors* – at the GO/FO/SES level – Validate and approve capability requirements documents; Provide senior

leadership and oversight of JCIDS analysis and staffing; Enforce capability requirements standards and accountability.

3. Training Courses. Courses created and administered by DAU for RMCT fall into two general categories.

3.1. Core courses. The RMCT required core courses are shown in Figure D-1.

TRAINING COURSE	CLR 101	RQM 110	RQM 310	RQM 403	RQM 413
TITLE	Introduction to JCIDS	Core Concepts for Requirements Management	Advanced Concepts and Skills	Requirements Executive Overview Workshop	Senior Leader Requirements Course
ESTIMATED TIME TO COMPLETE	4-6 Hours	18-24 Hours	1 Week	1 Day	Tailored
CERTIFICATION LEVEL	A, B, C	B, C	C	D (1-3 Star/SES)	D (4-Star/ Agency Head)

Figure D- 1: DAU-Administered RMCT Core Course Overview

3.1.1. CLR 101, Introduction to JCIDS. This on-line course provides an overview of the DoD capabilities analysis and requirements development process. The course focuses on terms, definitions, basic concepts, processes, and roles and responsibilities of personnel involved in executing the JCIDS process. Mandatory instruction for position categories A, B, & C. Prerequisites: none.

3.1.2. RQM 110, Core Concepts for Requirements Management. This on-line course covers both the requirements manager role and requirements management within the "Big A" acquisition construct. The course examines the capability development process from an end-to-end perspective, highlighting the interactions among JCIDS, DAS, and PPBE processes, with an emphasis on the requirements process. Mandatory instruction for position categories B & C. Prerequisites: CLR 101.

3.1.3. RQM 310, Advanced Concepts and Skills for Requirements Managers. This in-residence course is held at the DAU campus, DSMC, Fort Belvoir, VA. The course takes an in-depth look into the interactions among JCIDS, DAS, and PPBE processes, with an emphasis on the requirements process. Mandatory instruction for position category C. Prerequisites: RQM 110.

3.1.4. RQM 403, Requirements Executive Overview Workshop. This in-residence course, for GO/FO and SES personnel, provides an executive-level understanding of requirements management within the "Big A" acquisition construct. The course examines the capability development process from an end-to-end perspective, highlighting the interactions among JCIDS, DAS, and PPBE processes, as well as the role of the requirements manager, with an emphasis on the requirements process. Mandatory instruction for GO/FO and SES's in position category D. Prerequisites: none.

3.1.5. RQM 413, Senior Leader Requirements Course. This one-on-one course, focused on the 4-star Service Chief, Service Vice-Chief, CCMD Commander, Agency Director audience, provides senior leaders with an executive-level understanding of the interactions among JCIDS, DAS, and PPBE processes to meet the warfighters needs, with an emphasis on the requirements process. The presentation length and scope of the course is tailored to meet the needs of senior leaders. Prerequisites: none.

3.2. Core Plus courses. Core Plus courses are listed below in Figure D-2. These courses supplement the core curriculum and are not required for RMCT certification unless otherwise directed by DoD Component instruction and/or policy.

TRAINING COURSE	CLR 151	CLR 250	CLR 252	CLC 004
TITLE	Analysis of Alternatives	Capability Based Assessment	Developing Performance Attributes	Market Research
ESTIMATED TIME TO COMPLETE	3-5 Hours	3-5 Hours	3-5 Hours	3-5 Hours

Figure D- 2: DAU-Administered RMCT Core Plus Course Overview

3.2.1. CLR 151, Analysis of Alternatives (AoA). This on-line course provides professionals who lead or directly support AoAs with a comprehensive introduction to conducting AoA activities. Sponsors use the AoA to assess and prioritize potential materiel solutions and trade space in support of validated military capability requirements. Prerequisites: none, but CLR 101 is recommended for those without previous requirements experience.

3.2.2. CLR 250, Capabilities-Based Assessment (CBA). This on-line course provides professionals who lead or directly support CBAs with a comprehensive introduction to conducting CBA activities. Sponsors use the CBA to identify military capability requirements and associated capability gaps, as well as potential non-materiel and materiel approaches to close or mitigate capability gaps. Prerequisites: none, but CLR 101 is recommended for those without previous requirements experience.

3.2.3. CLR 252, Developing Performance Attributes. This on-line course provides professionals with instructions for developing high quality KPPs, KSAs, APAs, and other performance attributes, and the relationship of performance attributes to MOEs, MOPs, and measures of suitability. Prerequisites: none, but CLR 101 is recommended for those without previous requirements experience.

3.2.4. CLC-004 Market Research. This on-line course covers the function of market research for both products and services, teaches best practices for conduct of market research, and establishes a process for collecting and reporting market research results. Requirements Managers assigned to a market research team are required to take CLC-004, IAW Reference [158].

4. Course Attendance Guidelines.

4.1. Resident course attendance.

4.1.1. DAU receives funding to teach a number of students considered necessary to provide the requirements community with training directed by DoD senior leadership and Reference [157]. Each DoD Component receives a limited number of seats per year and should strive to fill all allocated seats with students in need of requirements training.

4.1.2. Component Appointed Representatives (CARs) will enroll prospective students in a course or add them to a course's official wait list only after verification that course pre-requisites have been completed by reviewing either/or:

4.1.2.1. Copy of student's DAU transcript.

4.1.2.2. Official DAU Course completion certificates for all pre-requisites.

4.2. Pre-course work. Any student scheduled to attend a DAU resident course is to thoroughly review the recommended and/or required preparatory pre-course work. Supervisors should ensure that their employees have sufficient time during the duty day to complete the pre-course work and provide assistance, if needed.

4.3. Walk-in students.

4.3.1. Documenting pre-requisite courses. Walk-in students NOT on the course waiting list will be required to provide documentation citing successful completion of prerequisite DAU course(s) as noted above for course enrollment. Walk-in students who are on the course waiting list do not need to provide documentation of pre-requisites, as they have already been verified.

4.3.2. Contractor attendance. Per Reference [159], contractors will be accepted into resident courses only on a walk-in basis, per DAU's walk-in regulations. Contractors may accomplish DAU on-line training as needed, subject to guidance and/or limitations in their contracts.

4.3.3. Priorities for filling open seats. Class seats remaining open due to low registration, short-notice cancellations, or course no-shows will be filled in the following priority order:

4.3.3.1. Military and DoD civilian students who work in requirements related billets and are on the course's official waiting list.

4.3.3.2. Military and DoD civilian students who work in non-requirements related billets, taking the course as a DAWIA Core-Plus or other knowledge broadening opportunity, and are on the course's official waiting list.

4.3.3.3. Military and DoD civilian students who work in requirements related billets and are walk-ins at the beginning of the course.

4.3.3.4. Military and DoD civilian students who work in non-requirements related billets, taking the course as a DAWIA Core-Plus or other knowledge broadening opportunity, and are walk-ins at the beginning of the course.

4.3.3.5. Contractor personnel who work in requirements related billets and are walk-ins at the beginning of the course.

4.3.3.6. Contractor personnel who are in non-requirements related billets, taking the course as a DAWIA Core-Plus or other knowledge broadening opportunity, and are walk-ins at the beginning of the course.

4.4. Course no-shows. Students who are enrolled in a resident course and fail to attend the class, impose a potential negative impact on the Component and seat allocations for future DAU courses.

4.4.1. Any no-show requirements community member(s) will remain ineligible to apply for future DAU courses for a period of four (4) months starting on the last day of the scheduled resident course for which they failed to appear.

4.4.2. The individual's supervisor and the first O-6, GS-15, or equivalent grade in the chain-of-command will sign a memorandum acknowledging the individual's no-show status. No later than 5 business days after first day of intended course, email the memorandum, Subject: No-Show, to the Center Director, Requirements Department, DSMC at RMCT@dau.mil.

4.5. Short notice cancellations. Cancellation within 14 days of the scheduled start date for resident courses is considered to be short notice. If a student cancels within the short notice timeframe, the student must inform his/her CAR as soon as possible. The CAR is responsible for filling the vacated slot with another student.

4.6. Course failures. A course failure can occur for numerous reasons including, but not limited to, students failing a graded event within a resident course, or students absent more than 5 percent of instructional time.

4.6.1. If such an instance occurs, the student must inform his/her supervisor and the first O-6, GS-15, or equivalent grade in the chain-of-command.

4.6.2. A memorandum acknowledging the individual's course failure must be written and signed by both the individual's supervisor and the first O-6, GS-15, or equivalent grade in the chain-of-command. Provide the memorandum to the Center Director, Requirements Department, DSMC, by sending the memorandum to RMCT@dau.mil, Subject: Course Failure.

4.7. Additional academic policies.

4.7.1. Reference [159] provides DAU's student academic policies and information for additional insight on DAU student matters not covered in this enclosure.

4.7.2. The Center Director, Requirements Department, DSMC, in consultation with the appropriate Component representative, may waive rules as they pertain to DAU's RMCT courses, curriculum, and any/all stipulations therein.

5. RMCT Management and Reporting.

5.1. RMCT Representatives. CARs and Functional Integrated Process Team (FIPT) representatives.

5.1.1. Each Component designates a Primary and Alternate CAR – typically O-4/O-5 or civilian equivalent – for day-to-day RMCT management activities. CAR oversight duties include, but are not limited to:

5.1.1.1. Identifying and tracking all billets/positions within the Component requiring training and certification IAW this enclosure.

5.1.1.2. Participating in FIPT working groups on behalf of the Component.

5.1.1.3. Requiring all personnel to participate in recurrent training in order to increase their skills and knowledge of the requirements process, and stay current IAW Reference [150]. In addition, encouraging participation in training related to the Defense Acquisition Workforce Improvement Act (DAWIA) career fields and functional areas detailed in Reference [160], is important to gain wider breadth of knowledge and understanding for the Defense Acquisition System.

5.1.2. Each Component designates a Functional Integrated Process Team (FIPT) leadership representative – typically O-6, GS-15, or equivalent grade – to represent the Component at RMCT leadership events. Primary duty of the FIPT Representative is to attend both the scheduled and unscheduled leadership forums and to have the authority to make decisions on behalf of the Component.

5.1.3. When designating or replacing a Primary and/or Alternate CAR or FIPT representative, send updated information to RMCT@dau.mil, Subject: CAR and/or FIPT Representative. Include first and last name, rank, Component, office name/symbol, email address, phone number, and specifically identify the individual(s) as the primary or alternate CAR or FIPT representative. Upon designation, a message will be sent from DAU to the individual with RMCT program details and expectations.

5.2. Requirements workforce status reports. When notified by a Joint Staff Action Processing (JSAP) task, not to exceed every 6 months, the CAR will submit a requirements workforce status report IAW JSAP instruction. The consolidation of JSAP Component responses will be briefed to the Requirements Management Functional Integrated Product Team (RM FIPT) and its senior steering group, the RM FIPT Tri-Chair. The Tri-Chair senior steering group includes the Functional Leader, Assistant Secretary of Defense for Acquisition (ASD(A)), Functional Advisor, JS/J-8 DDRCD, and the President, DAU. The JSAP responses are used to inform Congressional and DoD decision-makers on the status of the requirements workforce, allowing for

informed future training and resource allocation decisions. The JSAP responses will provide at a minimum the following information:

5.2.1. Number of RMCT Level 'B' Billets (Military/Civilian).

5.2.2. Number of RMCT Level 'C' Billets (Military/Civilian).

5.2.3. Number of RMCT Level 'D' Billets (Military/Civilian).

5.2.4. Number of Level 'B' Billets filled - trained/certified (Military/Civilian).

5.2.5. Number of Level 'C' Billets filled - trained/certified (Military/Civilian).

5.2.6. Number of Level 'D' Billets filled - trained/certified (Military/Civilian).

ENCLOSURE E

REFERENCES

[1] CJCSI 5123.01H, Charter of the Joint Requirements Oversight Council (JROC) and Implementation of the Joint Capabilities Integration and Development System (JCIDS), July 2018.

[2] Title 10 U.S.C. § 181, Joint Requirements Oversight Council.

[3] Joint Capabilities Integration and Development System Wiki, on NIPRNET - https://intellipedia.intelink.gov/wiki/Joint_Capabilities_Integration_and_Development_System, on SIPRNET - https://intellipedia.intelink.sgov.gov/wiki/JCIDS.

[4] Knowledge Management and Decision Support, on SIPRNET - https://jrockmdsbpm.js.smil.mil.

[5] DoDI 5000.02, Operation of the Defense Acquisition System, 7 January 2015, Incorporating Change 3, 10 August 2017.

[6] DoD CIO, DoD Architecture Framework (DoDAF) Version 2.02, on NIPRNET - http://dodcio.defense.gov/Library/DoD-Architecture-Framework, August 2010.

[7] Joint Staff J6 Warfighter Mission Area Architecture Federation and Integration Project Portal, on NIPRNET - https://wmaafip.csd.disa.mil, and on SIPRNET - https://wmaafip.csd.disa.smil.mil.

[8] UJTL Task Development Tool (UTDT), on NIPRNET - https://utdt.js.mil.

[9] DoDD 5000.01, The Defense Acquisition System, 12 May 2003.

[10] DoDI 8330.01, Interoperability of Information Technology (IT), Including National Security Systems (NSS), 21 May 2014, Incorporating Change 1, 18 December 2017.

[11] CJCSM 3265.01A, Joint Command and Control (C2) Requirements Management Process and Procedures, 29 November 2013.

[12] DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), Incorporating Change 2, 28 July 2017.

[13] Title 10 U.S.C. § 2448a, Program cost, fielding, and performance goals in planning major defense acquisition programs.

[14] Public Law 114-328 (FY17 NDAA), Section 925(b), Modifications to the Requirements Process, 23 December 2016.

[15] Title 10 U.S.C. § 2547, Acquisition-related functions of chiefs of the armed forces.

[16] United States Cyber Command Instruction (USCCI) , USCYBERCOM Cyber Capability Integration and Development System (C-CIDS).

[17] USSOCOM Directive 71-4, Special Operations Forces Capabilities Integration and Development System (SOFCIDS), 10 May 2012.

[18] JROCM 067-07, Funding Guidance for Joint Requirement Oversight Council Directed Actions, 23 March 2007.

[19] Title 10 U.S.C. § 2433a, Critical cost growth in major defense acquisition programs.

[20] AR 71-9, Warfighting Capabilities Determination, 28 December 2009.

[21] AF/A5R, Requirements Development Guidebook, Volume 2, Air Force Procedures: Urgent Needs, 20 March 2018, ver 7.1.

[22] SECNAVINST 5000.2E, Department of the Navy Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System, 1 September 2011.

[23] MCO 3900.17, The Marine Corps Urgent Needs Process (UNP) and Urgent Universal Needs Statement (Urgent UNS), 17 October 2008.

[24] TRADOC Regulation 71-20, Concept Development, Capabilities Determination, and Capabilities Integration, 28 June 2013.

[25] MCO 3900.20, Marine Corps Capabilities Based Assessment, 27 September 2016.

[26] DoDD 5000.71, Rapid Fulfillment of Combatant Commander Urgent Operational Needs, 24 August 2012.

[27] Intelligence Community Directive 115, Intelligence Community Capability Requirements Process, 21 December 2012.

[28] CJCSI 5250.01, Special Access Program (SAP) Policy, 15 February 2007, Current as of 8 November 2011 (Restricted Release).

[29] DoDD 5205.07, Special Access Program (SAP) Policy, 1 July 2010.

[30] AF/A5R, Requirements Development Guidebook, Volume 1, Policies and Guidelines, 20 March 2018, version 2.1.

[31] VCJCS and PDDNI Memorandum, Guidelines for Interaction between the Intelligence Community Capability Requirements Process and Joint Capabilities Integration and Development System, 30 July 2013.

[32] DJ-8 and DCMO Memorandum, Guidelines for Common Gatekeeping for the Acquisition of Defense Business Systems Documents and Interactions with the Joint Capabilities Integration and Development System Processes, 25 July 2014.

[33] DoDM 5200.01-V2, DoD Information Security Program: Marking of Classified Information, Incorporating Change 2, 19 March 2013.

[34] CJCSI 5714.01D, Policy for the Release of Joint Information, 18 April 2012.

[35] DIAD 5000.200, Intelligence Threat Support for Major Defense Acquisition Programs, 19 June 2018.

[36] DCMO, Defense Business Systems Investment Management Process Guidance, Version 4.0, April 2017.

[37] DoDI 5000.75, Business System Requirements and Acquisition, 2 February 2017.

[38] DoDI DoDI 4540.24.24, Operations of the DoD Engineering for Transportability and Deployability Program, 12 October 2004 including Change 1 of 11 September 2007.

[39] DoDI 2010.06, Materiel Interoperability and Standardization with Allies and Coalition Partners, 29 July 2009.

[40] DoDI 4120.24, Defense Standardization Program (DSP), 13 July 2011.

[41] DoDM 4120.24, Defense Standardization Program (DSP) Procedures, 24 September 2014.

[42] Content Guide for the Net-Ready KPP Wiki, On NIPRNET - https://intellipedia.intelink.gov/wiki/Content_Guide_for_the_Net-Ready_KPP.

[43] DoDI 8320.05, Electromagnetic Spectrum Data Sharing, Incorporating Change 1, 22 November 2017.

[44] DoDI 4650.01, Policy and Procedures for Management and Use of the Electromagnetic Spectrum, Incorporating Change 1, 17 October 2017.

[45] DoDD 5250.01, Management of Intelligence Mission Data (IMD) in Acquisition Data, Incorporating Change 1, 29 August 2017.

[46] JROCM 102-05, Safe Weapons in Joint Warfighting Environments, 20 May 2005.

[47] DoDI 5000.69, DoD Joint Services Weapon and Laser System Safety Review Processes, Incorporating Change 1, 20 November 2017.

[48] DoDI 5000.73, Cost Analysis Guidance and Procedures, 9 June 2015, Incorporating Change 1, 2 October 2017.

[49] USD(AT&L) Memorandum, Memorandum, Implementation Directive for Better Buying Power 2.0 - Achieving Greater Efficiency and Productivity in Defense Spending, 24 April 2013.

[50] Defense Acquisition Guidebook, Chapter 3-2, on NIPRNET - https://dag.dau.mil.

[51] Reliability, Availability, Maintainability, and Cost (RAM-C) Rationale Report Outline Guidance, 28 February 2017.

[52] DoDD 8000.01, Management of the Department of Defense Information Enterprise (DoD IE), Incorporating Change 1, 27 July 2017.

[53] JP 6-0, Joint Communications System, 10 June 2015.

[54] JROCM 095-09, Global Information Grid 2.0 Initial Capabilities Document, 1 June 2009.

[55] DoD 4650.1-R1, Link 16 Electromagnetic Compatibility (ECM) Feature Certification Process and Requirements, 26 April 2005.

[56] JROCM 057-18, 2018 Refinement of the Joint Capability Area Taxonomy and Definitions, 7 June 2018; JCA Taxonomy 2018; and JCA Definitions

2018; on NIPRNET - https://intellipedia.intelink.gov/wiki/Joint_Capability_Areas.

[57] Joint Mission Threads (JMT), on NIPRNET - https://wmaafip.csd.disa.mil/JMT/Home?aId=26&ptIDs=0.

[58] Joint Common System/Service Function List, on NIPRNET - https://intellipedia.intelink.gov/w/index.php?title=Joint_Common_System/Service_Function_List, and on SIPRNET - https://intellipedia.intelink.sgov.gov/wiki/Joint_Common_System/Service_Function_List.

[59] DoDI 8500.01, Cybersecurity, 14 March 2014.

[60] DoDI 8110.01, Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DoD, 25 September 2014.

[61] D. 8540.01, Cross Domain (CD) Policy, Incorporating Change 1, 28 August 2017.

[62] CJCSI 6285.01D, Mission Partner Environment Information Sharing Requirements Management Process, 21 August 2017.

[63] DoDI 8410.03, Network Management (NM), Incorporating Change 1, 19 July 2017.

[64] DoD Information Enterprise Architecture Version 2.0, on NIPRNET - http://dodcio.defense.gov/Home/Initiative/DIEA.aspx, 10 August 2012.

[65] CJCSI 3245.01B, All Domain-Overhead Cooperative Operations (AOCO), 22 January 2018.

[66] DoDI 3222.03, DoD Electromagnetic Environmental Effects (E3) Program, Incorporating Change 2, 10 October 2017.

[67] "Intelligence Community Joint Architecture Reference Model (IC JARM)," on NIPRNET - https://intellipedia.intelink.gov/wiki/Joint_Architecture_Working_Group.

[68] DoDI 4630.09, Communication Waveform Management and Standardization, Incorporating Change 1, 10 October 2017.

[69] DoDD 3222.04, Electronic Warfare (EW) Policy, Incorporating Change 1, 10 May 2017.

[70] DoDI 6055.15, DoD Laser Protection Program, 4 May 2007.

[71] DoDI 3150.09, The Chemical, Biological, Radiological, and Nuclear (CBRN) Survivability Policy, 8 April 2015, Incorporating Change 1, Effective 16 January 2018.

[72] DoDD S-5210.81, United States Nuclear Weapons Command and Control, Safety, and Security (U), Incorporating Change 1, 11 September 2015.

[73] DoDI 6055.01, DoD Safety and Occupational Health (SOH) Program, 14 October 2014.

[74] MIL-STD-1472G, Department of Defense Design Criteria Standard - Human Engineering, 11 January 2012.

[75] JSSG-2010-10, Department of Defense Joint Service Specification Guide - Crew Systems Oxygen Systems Handbook, 30 October 1998.

[76] Title 29 CFR § 1910.95, Occupational noise exposure.

[77] JSSG-2010-7, Department of Defense Joint Service Specification Guide - Crew Systems Crash Protection Handbook, 30 October 1998.

[78] DoDD 3100.10, Space Policy, Incorporating Change 1, 4 November 2016.

[79] OSD/CAPE, Operating and Support Cost-Estimating Guide, March 2014.

[80] CJCSI 5120.02D, Joint Doctine Development System, 5 January 2015.

[81] CJCSI 4320.01E, Requirement Authorization Documents for Joint Organizations, Joint Task Forces, Standing Joint Force Headquarters, and Other Joint Organizations, 21 August 2014.

[82] CJCSI 3500.01H, Joint Training Policy for the Armed Forces of the United States, 25 April 2014.

[83] CJCSI 1800.01E, Officer Professional Military Education Policy, 29 May 2015.

[84] CJCSI 1805.01B, Enlisted Professional Military Education Policy, 15 May 2015.

[85] CJCSI 1001.01B, Joint Manpower and Personnel Program, 7 October 2014.

[86] DoDD 4165.06, Real Property, 13 October 2004, Certified Current 18 November 2008.

[87] DoDI 4165.03, DoD Real Property Categorization, 24 August 2012, Incorporating Change 2, 5 October 2017.

[88] DoDI 4165.70, Real Property Management, 6 April 2005.

[89] DoDI 5111.16, Policy and Strategy Committee, 27 October 2005.

[90] DoD Dictionary of Military and Associated Terms, As of March 2018.

[91] USD(P&R), Strategic Plan for the Next Generation of Training for the Department of Defense, 23 September 2010.

[92] DoDD 1322.18, Military Training, Incorporating Change 1, 23 February 2017.

[93] CJCSI 3901.01E, Requirements for Geospatial Information and Services, 28 November 2016.

[94] DoDI 5000.56, Programming Geospatial Intelligence (GEOINT), Geospatial Information and Services (GI&S), and Geodesy Requirements for Developing Systems, 9 July 2010, Incorporating Change 1, 25 September 2017.

[95] CJCSI 6130.01F, 2016 Chairman of the Joint Chiefs of Staff Master Positioning, Navigation, and Timing Plan, 30 September 2016.

[96] JP 2-0, Joint Intelligence, 22 October 2013.

[97] NSGM 3202, The GEOINT Functional Manager Standards Assessment (GFMSA) Program, 9 June 2016.

[98] NSGD 3201, The Geospatial Intelligence (GEOINT) Functional Manager Standards Assessment (GFMSA) Program, Change 1, 19 November 2015.

[99] DoDI 8310.01, Information Technology Standards in the DoD, Incorporating Change 1, 31 July 2017.

[100] Intelligence Community Directive 503, Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation, 15 September 2008.

[101] Intelligence Community Directive 705, Sensitive Compartmented Information Facilities, 26 May 2010.

[102] JP 3-60, Joint Targeting, 31 January 2013.

[103] CJCSI 3505.01C, Target Coordinate Mensuration Certification and Program Accreditation, 28 October 2016.

[104] DIA Intelligence Mission Data Center SharePoint Site, on SIPRNET - https://intelshare.intelink.sgov.gov/sites/imdc/lmdppublicshare/default.aspx.

[105] JP 3-14, Space Operations, 29 May 2013.

[106] JP 2-01.2, Counterintelligence and Human Intelligence in Joint Operations, 6 April 2016.

[107] DoDI O-5240.24, Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA), Incorporating Change 1, 15 October 2013.

[108] DoDI 5200.39, Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E), Incorporating Change 1, 17 November 2017.

[109] DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN), Incorporating Change 2, 27 July 2017.

[110] MLS-STD-882E, Department of Defense Standard Practice for System Safety, 11 May 2012.

[111] JROCM 235-06, Insensitive Munitions Standards and Passing Criteria, 6 November 2006.

[112] MIL-STD-2105D, Department of Defense Test Method Standard - Hazard Assessment Tests for Non-Nuclear Munitions, 19 April 2011.

[113] MIL-STD-1316F, Department of Defense Design Criteria Standard - Fuze Design, Safety Criteria for, 18 August 2017.

[114] JOTP-051, Technical ManuDepartment of Defense Joint Ordnance Test Procedure (JOTP) - Technical Manual for the Use of Logic Devices in Safety Featuresal for the Use of Logic Devices in Safety Features, 10 February 2012.

[115] JOTP-052, Department of Defense Joint Ordnance Test Procedure (JOTP) - Guideline for Qualification of Fuzes, Safe and Arm (S&A) Devices, and Ignition Safety Devices (ISD), 17 March 2012.

[116] DoDD 5160.62, Single Manager Responsibility for Military Explosive Ordnance Disposal Technology and Training (EODT&T), Incorporating Change 1, 15 May 2017.

[117] MIL-STD-464C, Department of Defense Interface Standard - Electromagnetic Environment Effects Requirements for Systems, 1 December 2010.

[118] MIL-STD-461G, Department of Defense Interface Standard - Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment, 11 December 2015.

[119] DoDM 6055.09 (Volumes 1-8), DoD Ammunition and Explosives Safety Standards, 29 February 2008, incorporating changes of various dates by volume.

[120] JROC KMDS Knowledge Management and Decision Support Wiki, on SIPRNET - https://intellipedia.intelink.sgov.gov/wiki/Portal: JROC_KMDS_Knowledge_Management_and_Decision_Support.

[121] Defense Acquisition Management Information Retrieval (DAMIR), on NIPRNET - https://ebiz.acq.osd.mil/DAMIR/PortalMain/DamirPortal.aspx.

[122] DoDI 3200.12, DoD Scientific and Technical Information Program (STIP), 22 August 2013.

[123] DTIC, Unified Research and Engineering Database, on NIPRNET - https://www.dodtechipedia.mil/dodwiki/pages/viewpage.action?pageId =73796052.

[124] CJCSM 3130.06B, Global Force Management Allocation Policies and Procedures, 12 October 2016 (Secret Document).

[125] DoDD 7730.65, Department of Defense Readiness Reporting System (DRRS), Incorporating Change 1, 31 May 2018.

[126] CJCSI 3401.02B, Force Readiness Reporting, 31 May 2011.

[127] DoDI 3000.04, DoD Munitions Requirements Process (MRP), 24 September 2009.

[128] DoDD 7045.14, The Planning, Programming, Budgeting, and Execution (PPBE) Process, Incorporating Change 1, 29 August 2017.

[129] DoD 7000.14 - R, Department of Defense Financial Management Regulation, June 2017, on NIPRNET - http://comptroller.defense.gov/FMR.

[130] CJCSI 3100.01C, Joint Strategic Planning System, 20 November 2015.

[131] CJCSI 3010.02E, Guidance for Developing and Implementing Joint Concepts, 17 August 2016.

[132] CJCSI 3401.01E, Joint Combat Capability Assessment, 13 April 2010.

[133] CJCSI 3460.01C, Combat Support Agency Review Team Assessments, 9 August 2012.

[134] DoDI 8260.03, The Global Force Management Data Initiative (GFM DI), Incorporating Change 1, 19 March 2018.

[135] Title 10 U.S.C. § 153, Chairman: functions.

[136] Title 10 U.S.C. § 166, Combatant commands: budget proposals.

[137] Joint Staff, Capability Gap Assessment (CGA) FY20-24 Guide, Change 1, June 2017, on SIPRNET - https://intellipedia/intelink.sgov.gov/w/images/a/af/CGA_Guide_FY20-24_Change_1.pdf.

[138] CJCSI 3150.25G, Joint Lessons Learned Program, 31 January 2018.

[139] JCS J-8/Force Structure, Resources, and Assessments Directorate, Capabilities-Based Assessment (CBA) User's Guide, Version 3, March 2009.

[140] TRADOC, Capabilities-Based Assessment (CBA) Guide, Version 3.1, 10 May 2010.

[141] AFMC/OAS, Pre-Materiel Development Decision (MDD) Analysis Handbook: A Practical Guide for Analyses from Capabilities Based Planning to Materiel Development Decision, July 2010.

[142] CJCSM 3122.01A, Joint Operation Planning and Execution System (JOPES) Volume I, Planning Policies and Procedures, 29 September 2006, Current as of 13 November 2014.

[143] CJCSM 3122.02D, Joint Operation Planning and Execution System (JOPES) Volume III Time-Phased Force and Deployment Data Development and Deployment Execution, Change 1, 21 May 2015.

[144] CJCSM 3130.01A, Campaign Planning Procedures and Responsibilities, 25 November 2014.

[145] JP 5-0, Joint Planning, 16 June 2017.

[146] CJCSM 3150.25A, Joint Lessons Learned Program, 12 September 2014.

[147] Joint Capability Technology Demonstration Office, on NIPRNET - https://www.acq.osd.mil/ecp/PROGRAMS/JCTD.html.

[148] Global Force Management Board Wiki, on SIPRNET - https://intellipedia.intelink.sgov.gov/wiki/Global_Force_Management_Board.

[149] Title 10 U.S.C. § 2330, Procurement of contract services: management structure.

[150] AFMC/OAS, Analysis of Alternatives (AoA) Handbook: A Practical Guide to the Analyses of Alternatives, 10 June 2013.

[151] DoDI 8260.2, Implementation of Data Collection, Development, and Management for Strategic Analyses, 21 January 2003.

[152] DoDD 8260.05, Support for Strategic Analysis (SSA), 7 July 2011.

[153] DIA/TLA, DIA Defense Technology and Long-Range Analysis Office Acquisition Threat Support Division Wiki, on SIPRNET - https://intellipedia.intelink.sgov.gov/wiki/TLA-3.

[154] CJCSM 3500.04F, Universal Joint Task Manual, 1 June 2011.

[155] JROCM 167-03, Joint Command and Control (JC2) Operational Requirements Document (ORD), 22 August 2003.

[156] USD(I) Memorandum, Defense Intelligence Information Enterprise (DIIE (now DI2E)) Way Ahead, 3 October 2009.

[157] Public Law 109-364 (FY07 NDAA), Section 801, Requirements Management Certification Training Program, 17 October 2006.

[158] Public Law 114-92 (FY16 NDAA), Section 844, "Mandatory Requirement for Training Related to the Conduct of Market Research," 25 November 2015.

[159] DAU, Student Policies & Info, on NIPRNET - https://www.dau.mil/training/p/Student-Policies-Info.

[160] Defense Acquisition University, on NIPRNET - https://dap.dau.mil.

(INTENTIONALY BLANK)

GLOSSARY

1. PART I - ABBREVIATIONS AND ACRONYMS

A2/AD	Anti-Access/Area Denial
ACAT	Acquisition Category
ACCM	Alternative Compensatory Control Measure
Acq	Acquisition
ADM	Acquisition Decision Memorandum
ADNI/SRA	Associate Director of National Intelligence for Systems and Resource Analysis
AF/A5R	Air Force Directorate of Operational Requirements
AFATDS	Advanced Field Artillery Tactical Data System
AFMC	Air Force Materiel Command
AJA	Annual Joint Assessment
ALDT	Administrative and Logistics Downtime
Am	Materiel Availability
Ao	Operational Availability
AO	Action Officer
AoA	Analysis of Alternatives
AOCO	All Domain-Overhead Cooperative Operations
AOR	Area of Responsibility
APA	Additional Performance Attribute
APB	Acquisition Program Baseline
APUC	Average Procurement Unit Cost
AR	Army Regulation
ASD(R&E)	Assistant Secretary of Defense for Research and Engineering
AV-#	(DoDAF) All Viewpoint
BA	Battlespace Awareness (FCB or JCA)
BCAC	Business Capability Acquisition Cycle
BDA	Battle Damage Assessment
BES	Budget Estimate Submission
BFT	Blue Force Tracking
BIT	Built-In Test
BY	Base Year
C&P	Characteristics and Performance
C2	Command and Control
C3	Command, Control, and Communications
C4	Command, Control, Communications, and Computers
CAC	Common Access Card
CAD	Capabilities and Acquisition Division (in J-8)
CAE	Component Acquisition Executive
CAIV	Cost As an Independent Variable

CAPE	Cost Assessment and Program Evaluation
CAR	Component Appointed Representative
CARD	Cost Analysis Requirements Data
CASREP	Casualty Report
CBA	Capabilities-Based Assessment
CBP	Capabilities-Based Planning
CBRN	Chemical, Biological, Radiological, and Nuclear
CCDR	Combatant Commander
CCIF	CCMD Initiatives Fund
CCJO	Capstone Concept for Joint Operations
CCMD	Combatant Command
CD	Capability Drop
CD	Cross Domain
CDD	Capability Development Document
CDR	Critical Design Review
CFR	Code of Federal Regulations
CGA	Capability Gap Assessment
CI	Counterintelligence
CICA	Classified Information Compromise Assessment
CIP	Critical Intelligence Parameter
CISP	Counterintelligence Support Plan
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CLC	DAU Continuous Learning Module for Contracts
CLR	DAU Continuous Learning Module for Requirements
CML	Capability-Mission Lattice
CNGB	Chief, National Guard Bureau
CO	Cyberspace Operations
COI	Community of Interest
COLISEUM	Community On-Line Intelligence System for End Users and Managers
COMINT	Communications Intelligence
CONOPS	Concept of Operations
CONPLAN	Concept Plan
CO-P	Cyber Operations Peculiar
COTS	Commercial Off-the-Shelf
CP	Capability Package
CPA	Chairman's Program Assessment
CPD	Capability Production Document
CPI	Critical Program Information
CPM	Capability Portfolio Management
CPMR	Capability Portfolio Management Review
CPR	Chairman's Program Recommendation

CRA	Chairman's Risk Assessment
CRIB	USCYBERCOM Requirements and Investment Board
CSA	Combat Support Agency
CSA	Cyber Survivability Attribute
CSE	Cyber Survivability Endorsement
CSEIG	Cyber Survivability Endorsement Implementation Guide
CSRC	Cyber Survivability Risk Category
CTA	Capstone Threat Assessment
CTC	Combat Training Center
CV-#	(DoDAF) Capability Viewpoint
DAB	Defense Acquisition Board
DAES	Defense Acquisition Executive Summary
DAMIR	Defense Acquisition Management Information Retrieval
DAR	Defense Acquisition Report
DAS	Defense Acquisition System
DASD(MR)	Deputy Assistant Secretary of Defense for Materiel Readiness
DASD(OE)	Deputy Assistant Secretary of Defense for Operational Energy
DAU	Defense Acquisition University
DAWIA	Defense Acquisition Workforce Improvement Act
DBC	Defense Business Council
DBS	Defense Business System
DCMO	Deputy Chief Management Officer
DCNO	Deputy Chief of Naval Operations
DCR	DOTmLPF-P Change Recommendation
DDC4Cyber	Deputy Director for Command, Control, Communications, & Computers/Cyber (in J-6)
DDC5I	Deputy Director for Command, Control, Communications, Computers, and Cyber Integration (in J-6)
DDFP	Deputy Director for Force Protection (in J-8)
DDJED	Joint Staff J-7 Deputy Director, Joint Education and Doctrine
DDMS	DoD Discovery Metadata Specification
DDOL(M)	Joint Staff J-4, Deputy Director for Operational Logistics (Maintenance)
DDRA	Deputy Director for Resources and Acquisition (in J-8)
DDRCD	Deputy Director for Requirements and Capability Development (in J-8)
DDSA	Deputy Director for Studies and Analysis (in J-8)
DI	Data Initiative

DI2E	Defense Intelligence Information Environment (formerly DIIE)
DIA	Defense Intelligence Agency
DIA/TLA	Defense Intelligence Agency Defense Technology and Long-Range Analysis Office
DIAAE	Defense Intelligence All-Source Analysis Enterprise
DIAD	Defense Intelligence Agency Directive
DIRINT	Director of Intelligence
DISR	DoD Information Technology Standards Registry
DITL	Defense Intelligence Threat Library
DIV-#	(DoDAF) Data and Information Viewpoint
DJ-2	Director, Joint Staff J-2 Directorate for Intelligence
DJ-4	Director, Joint Staff J-4 Directorate for Logistics
DJ-7	Director, Joint Staff J-7 Directorate for Joint Force Development
DJ-8	Director, Joint Staff J-8 Directorate for Force Structure, Resources, and Assessment
DNI	Director of National Intelligence
DO	Directorate for Operations
DoD	Department of Defense
DoD CIO	DoD Chief Information Officer
DoD IEA	DoD Information Enterprise Architecture
DoDAF	DoD Architecture Framework
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDIN	DoD Information Network
DoDM	Department of Defense Manual
DOT&E	Director of Operational Test and Evaluation
DOTmLPF-P	Doctrine, Organization, Training, materiel, Leadership and Education, Personnel, Facilities, and Policy
DPG	Defense Planning Guidance
DRRS	Defense Readiness Reporting System
DSMC	Defense Systems Management College
DSN	Defense Switching Network
DT	Dwell Time
DTED	Digital Terrain Elevation Data
DTIC	Defense Technical Information Center
DUSD(A&T)	Deputy Under Secretary of Defense for Acquisition and Technology
E3	Electromagnetic Environmental Effects
EA	Electronic Attack
ECM	Electromagnetic Compatibility
ECS&D	Enterprise Content Search and Discovery
ED	Engineering Division (in J-4)

ELINT	Electronic Intelligence
EM	Electromagnetic
EMD	Engineering and Manufacturing Development (Phase of Acquisition)
EME	Electromagnetic Operating Environment
EMP	Electromagnetic Pulse
EMSO	Electromagnetic Spectrum Operations
EMV	Electromagnetic Vulnerability
EODT&T	Explosive Ordnance Disposal Technology and Training
EP	Electronic Protection
ESD	Electrostatic Discharge
ESOH	Environment, Safety, and Occupational Health
EW	Electronic Warfare
EWIR	Electronic Warfare Integrated Reprogramming
FA	Force Application (FCB or JCA)
FCB	Functional Capabilities Board
FCB WG	FCB Working Group
FD	Forces Division (in J-8))
FDD	Full Deployment Decision
FIPT	Functional IPT
FISINT	Foreign Instrumentation Signals Intelligence
FMV	Full Motion Video
FOC	Full Operational Capability
FoJC	Family of Joint Concepts
FoS	Family of Systems
FP	Force Protection (KPP)
FPD	Force Protection Division (in J-8)
FPO	Functional Process Owner
ft3	Cubic Feet
FUE	First Unit Equipped
FY	Fiscal Year
FYDP	Future Years Defense Program
G2	Army Intelligence
GEF	Guidance for the Employment of the Force
GEOINT	Geospatial Intelligence
GFM	Global Force Management
GFMAP	Global Force Management Allocation Process
GFMB	Global Force Management Board
GFMIG	Global Force Management Implementation Guidance
GFMSA	GEOINT Functional Manager Standards Assessment
GI&S	Geospatial Information and Services
GO/FO	General Officer/Flag Officer
GOTS	Government Off-the-Shelf

GS	Government Service
GSA	GFMAP Sufficiency Assessment
GSD	Ground Sample Distance
HEMP	High Altitude Electromagnetic Pulse
HERF	Hazards of Electromagnetic Radiation to Fuels
HERO	Hazards of Electromagnetic Radiation to Ordnance
HERP	Hazards of Electromagnetic Radiation to Personnel
HQDA	Headquarters, Department of the Army
Hrs	Hours
HSI	Human Systems Integration
HUMINT	Human Intelligence
HVT	High Value Target
I&S	Interoperability and Supportability
IA	Information Assurance
IAM	Acquisition Category I for Major Automated Information Systems (as in ACAT IAM)
IC	Intelligence Community
IC	International Cooperation
ICCR	Intelligence Community Capability Requirements
ICD	Initial Capabilities Document
ICE	Independent Cost Estimate
ICMR	Intelligence Community Metadata Repository
ICTO	Interim Certificate to Operate
ID	Acquisition Category I Defense Acquisition Executive (DAE) (as in ACAT ID)
IE	Information Enterprise
IED	Improvised Explosive Device
IM	Insensitive Munition
IMD	Intelligence Mission Data
IMDC	Intelligence Mission Data Center
IOC	Initial Operational Capability
IPL	Integrated Priority List
IPOE	Intelligence Preparation of the Operational Environment
IPT	Integrated Process Teams
IRCO	Intelligence Requirements Certification Office (in J-283)
IRP	Investment Review Process
IS	Information Systems
ISA	Intelligence Supportability Analysis
ISC	Integrated Security Construct
IS-CDD	Information Systems Capability Development Document
ISD	Ignition Safety Device

ISP	Information Support Plan
ISR	Intelligence, Surveillance, and Reconnaissance
ISSA	Intelligence Sensitivity Systems Assessment
IT	Information Technology
ITEA	Initial Threat Environment Assessment
J-1	Joint Staff Directorate for Manpower and Personnel
J-2	Joint Staff Directorate for Intelligence
J-4	Joint Staff Directorate for Logistics
J-5	Joint Staff Directorate for Strategic Plans and Policy
J-6	Joint Staff Directorate for Command, Control, Communications, & Computers/Cyber
J-6/C4Cyber	Joint Staff Deputy Director for C4/Cyber
J-7	Joint Staff Directorate for Joint Force Development
J-8	Joint Staff Directorate for Force Structure, Resources, and Assessment
JARM	Joint Architecture Reference Model
JC2	Joint Command and Control
JCA	Joint Capability Area
JCAMP	Joint Capability Area Management Plan
JCB	Joint Capabilities Board
JCCA	Joint Combat Capability Assessment
JCD	Joint Capabilities Division (in J-8)
JCD	Joint Concept Development
JCIDS	Joint Capabilities Integration and Development System
JCSFL	Joint Common System Function List
JCTD	Joint Capability Technology Demonstration
JDEIS	Joint Doctrine, Education, & Training Electronic Information System
JDIR	Joint Staff Director
JEON	Joint Emergent Operational Need
JFP	Joint Force Provider
JIB	JCIDS Integration Branch (in J-7)
JIE	Joint Intelligence Estimate
JIE ORA	Joint Information Environment Operational Reference Architecture
JIPOE	Joint Intelligence Preparation of the Operational Environment
JITC	Joint Interoperability Test Command
JLE	Joint Logistics Estimate
JLLIS	Joint Lessons Learned Information System
JMETL	Joint Mission Essential Task List
JMT	Joint Mission Thread
JMVP	Joint Manpower Validation Process

JOPES	Joint Operation Planning and Execution System
JOTP	Joint Ordnance Test Procedure
JP	Joint Publication
JPE	Joint Personnel Estimate
JPME	Joint Professional Military Education
JPMED	Joint Professional Military Education (in J-7)
JPR	Joint Performance Requirement
JRAC	Joint Rapid Acquisition Cell
JROC	Joint Requirements Oversight Council
JROCM	Joint Requirements Oversight Council Memorandum
JS	Joint Staff
JSA	Joint Strategic Assessment
JSAP	Joint Staff Action Processing (task)
JSCP	Joint Strategic Capabilities Plan
JSD	Joint Staffing Designator
JSM	Joint Staff Manual
JSPS	Joint Strategic Planning System
JSR	Joint Strategic Review
JSSG	Joint Service Specification Guide
JTRS	Joint Tactical Radio System
JUON	Joint Urgent Operational Need
JWICS	Joint Worldwide Intelligence Communications System
JWSTAP	Joint Weapons Safety Technical Advisory Panel
KM/DS	Knowledge Management and Decision Support
KPP	Key Performance Parameter
KSA	Key System Attribute
kW	Kilowatt
LCAC	Landing Craft Air Cushion
LCCE	Lifecycle Cost Estimate
LMDP	Lifecycle Mission Data Plan
LTG	Lieutenant General (U.S. Army)
M&S	Modeling and Simulation
MAIS	Major Automated Information System
MASINT	Measurement and Signature Intelligence
MCO	Major Combat Operation
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MDCO	Military Department CI Organization
MDD	Materiel Development Decision
MDF	Mission Data File
MDT	Mean Down Time
MEA	Munitions Effects Assessment
MEF	Mission Essential Functions
MER	Manpower Estimation Report

METOC	Meteorological and Oceanographic
MIB	Military Intelligence Board
MILCON	Military Construction
MILPERS	Military Personnel
MIP	Military Intelligence Program
MMSD	Maintenance, Materiel, and Services Division (in J-4)
MOE	Measure of Effectiveness
MOP	Measure of Performance
MOSA	Modular Open System Approach
MPE	Mission Partner Environment
MRA	Manufacturing Readiness Assessment
MRP	Munitions Requirements Process
MS	Milestone
MSA	Materiel Solution Analysis (Phase of Acquisition)
MSFD	Multi-Service Force Deployment
MT	Mission Thread
MTBCF	Mean Time Between Critical Failures
MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair
N.n	Reference to JCA TIER N, Sub-Tier n
N2/N6	DCNO for Information Dominance
NDAA	National Defense Authorization Act
NDI	Non-Developmental Item
NDS	National Defense Strategy
NETOPS	Network Operations
NGA	National Geospatial-Intelligence Agency
NIIRS	National Imagery Interpretability Rating Scale
NIP	National Intelligence Program
NIPRNET	Non-secure Internet Protocol Router Network
NM	Network Management
NMS	National Military Strategy
NSA	National Security Agency
NSG	National System for Geospatial Intelligence
NSGD	NSG Directive
NSGM	NSG Manual
NSS	National Security Strategy
NSS	National Security System
NWC	Nuclear Weapons Council
O&M	Operation and Maintenance
O&S	Operations and Support (Phase of Acquisition)
OARL	Operating At Risk List
OAS	Office of Aerospace Studies
OASD(L&MR)	Office of the Assistant Secretary of Defense for Logistics & Materiel Readiness

OCA	Original Classification Authority
OCI	Office of Counterintelligence (in DIA/DO)
OCMO	Office of the Chief Management Officer
OCONUS	Outside Continental United States
OCR	Office of Collateral Responsibility
OEPP	Operational Energy Plans and Programs (ASD(OEPP))
OIPT	Overarching Integrated Process Team
OMB	Office of Management and Budget
OMS/MP	Operational Mode Summary/Mission Profile
OOB	Order of Battle
OPLAN	Operation Plan
OPR	Office of Primary Responsibility
ORD	Operational Requirements Document
OSD	Office of the Secretary of Defense
OT&E	Operational Test and Evaluation
OV-#	(DoDAF) Operational Viewpoint
P	Program Office (in Figure B-20)
P&D	Production and Deployment (Phase of Acquisition)
PAUC	Program Acquisition Unit Cost
PBAD	Program and Budget Analysis Division (in J-8)
PBR	Program and Budget Review
PDDNI	Principal Deputy Director of National Intelligence
PDM	Program Decision Memorandum
PDR	Preliminary Design Review
PDUSD(P)	Principle Deputy Under Secretary of Defense for Policy
PED	Processing, Exploitation, and Dissemination
PEO	Program Executive Officer
PES	Physical Exchange Specification
PIIT	Platform Integration Information Table
PIT	Platform Information Technology
PKI	Public Key Infrastructure
PM	Program Manager
PNT	Positioning, Navigation, and Timing
POA&M	Plan of Action and Milestones
POC	Point of Contact
POM	Program Objective Memorandum
POR	Program of Record
PPBE	Planning, Programming, Budgeting, and Execution
PPD	Policy and Programs Division (in J-7)
PPP	Program Protection Plan
PR	Performance Requirement
PSA	Principal Staff Assistant
PV-#	(DoDAF) Project Viewpoint
QDR	Quadrennial Defense Review

QRM	Quadrennial Roles and Missions
RAM-C	Reliability, Availability, Maintainability, and Cost
RDA	Research, Development, and Acquisition
RDP	Requirements Definition Package
RDT&E	Research, Development, Test, and Evaluation
RF	Radio Frequency
RFC	Request for Capabilities
RFF	Request for Forces
RFP	Request for Proposal
RMCT	Requirements Management Certification Training
RMF	Risk Management Framework
RPD	Requirements Definition Package
RQM	Requirements Management
S	Sponsor (See Figure A-4 and Figure B-20)
S&A	Safe and Arm
S&T	Science and Technology
S/P	Sponsor/Program Office (See Figure A-4 and Figure B-20)
SAASM	Selective Availability Anti-Spoofing Module
SAP	Special Access Program
SAPCO	Special Access Program Control Office
SAPCOORD	Special Access Program Coordinator (in J-8)
SAR	Selected Acquisition Report
SAR	Special Access Required
SATCOM	Satellite Communication
SCI	Sensitive Compartmented Information
SecDef	Secretary of Defense
SECNAVINST	Secretary of the Navy Instruction
SEP	Systems Engineering Plan
SES	Senior Executive Service
SIG	Senior Integration Group
SIGINT	Signals Intelligence
SIPRNET	Secure Internet Protocol Router Network
SME	Subject Matter Expert
SOFCIDS	Special Operations Forces Capabilities Integration and Development System
SOH	Safety and Occupational Health
SoN	Safety of Navigation
SO-P	Special Operations Peculiar
SoS	System of Systems
SRSA	Strategic Requirements Sufficiency Assessment (formerly known as the Joint Force Assessment)
SS	System Survivability (KSA)
SSA	Spectrum Survivability Attribute

SSA	Support for Strategic Analysis
SSP	System Safety Program
SSRA	Spectrum Supportability Risk Assessment
STA	System Threat Assessment
STANAGs	Standardization Agreements
STAR	System Threat Assessment Report
StdV-#	(DoDAF) Standards Viewpoint
STIP	Scientific and Technical Information Program
SV-#	(DoDAF) Systems Viewpoint
SvcV-#	(DoDAF) Services Viewpoint
SWAP-C	Space, Weight, Power, and Cooling
T&E	Test and Evaluation
TDL	Tactical Data Link
TEMP	Test and Evaluation Master Plan
TLA	Technology and Long Range Analysis Office (Reference DIA/TLA)
TMRR	Technology Maturation and Risk Reduction
TOA	Total Obligation Authority
TOC	Total Ownership Cost
TOS	Time on Station
TRA	Technology Readiness Assessment
TRADOC	U.S. Army Training and Doctrine Command
TRL	Technology Readiness Level
TS	Top Secret
TSN	Trusted Systems and Networks
TTPs	Tactics, Techniques, and Procedures
TTRA	Technology Targeting Risk Assessment
U.S.C.	United States Code
UAV	Unmanned Aerial Vehicle
UCP	Unified Command Plan
UDTD	UJTL Task Development Tool
UJT	Universal Joint Task
UJTL	Universal Joint Task List
UNP	Urgent Needs Process
UNS	Urgent Needs Statement
UON	Urgent Operational Need
URL	Uniform Resource Locator
USCENTCOM	United States Central Command
USCYBERCOM	United States Cyber Command
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(C)	Under Secretary of Defense (Comptroller)
USD(I)	Under Secretary of Defense for Intelligence

USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USD(P)	Under Secretary of Defense for Policy
USD(R&E)	Under Secretary of Defense for Research and Engineering
USSOCOM	United States Special Operations Command
UXO	Unexploded Ordnance
VCJCS	Vice Chairman of the Joint Chiefs of Staff
VOLT	Validated Online Lifecycle Threat
VTC	Video Teleconference
WARM	Wartime Reserve Mode
WEA	Warfighting Enterprise Architecture
WIN-T	Warfighter Information Network-Tactical
WMA	Warfighter Mission Area
WMA-AFIP	WMA Architecture Federation and Integration Portal
WSE	Weapon Safety Endorsement
W-SIG	Warfighter Senior Integration Group

(INTENTIONALLY BLANK)

2. PART II - DEFINITIONS

Unless otherwise stated, the terms and definitions contained in this glossary are for the purposes of this manual only.

Automated Information Systems - 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 an integral part of a weapon or weapon system; used for highly sensitive classified programs (as determined by the Secretary of Defense); used for other highly sensitive information technology (IT) programs (as determined by the DoD CIO); or determined by the DAE 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). (Source: DoDI 5000.02)

Capability - The ability to complete a task or execute a course of action under specified conditions and level of performance. (Source: DoD Dictionary of Military and Associated Terms)

Capability Drop - This describes the performance characteristics of a relatively small increment of a capability solution included in a software build necessary for partial deployment of the overall capability solution, typically developed and fielded within a short period of time. It could be developed through a rapid prototyping effort with the user to ensure it meets their needs. A CD (or equivalent) could be developed directly from the definitions in the IS-CDD in the event of a more timely need for the capability solution. More commonly, multiple CDs (or equivalents) would be derived from an RDP (or equivalent) or IS-CDD to deliver the overall capability solution defined in the RDP (or equivalent) or IS-CDD. (Source: JCIDS Manual)

Capability Gap - The inability to meet or exceed a capability requirement, resulting in an associated operational risk until closed or mitigated. The gap may be the result of no fielded capability, lack of proficiency or sufficiency in a fielded capability solution, or the need to replace a fielded capability solution to prevent a future gap. (Source: CJCSI 5123.01)

Capability Gap Assessment (CGA) – A deliberate assessment of the future year's defense program that reviews CCMD IPLs and other issues and perspectives from the Services and other DoD Agencies, relative to fielded materiel and non-materiel capability solutions, and development efforts which may already be underway to address capability gaps. (Source: CJCSI 5123.01)

Capability Need - See "Capability Requirement."

Capability Requirement - A capability which is needed to meet an organization's roles, functions, and missions in current or future operations. To the greatest extent possible, capability requirements are described in

relation to tasks, standards, and conditions IAW the Universal Joint Task List or equivalent DoD Component Task List. If a capability requirement is not satisfied by a capability solution, then there is also an associated capability gap. A requirement is considered to be 'draft' or 'proposed' until validated by the appropriate authority. (Source: CJCSI 5123.01)

Capability Requirements document – Any document used to articulate either deliberate or urgent/emergent capability requirements and associated information pertinent to review and validation. (Source: CJCSI 5123.01)

Capability Solution - A materiel solution or non-materiel solution to satisfy one or more capability requirements and reduce or eliminate one or more capability gaps. (Source: CJCSI 5123.01)

Contingency Operation - A military operation that (a) is designated by the SecDef as an operation in which members of the armed forces are or may become involved in military actions, operations, or hostilities against an enemy of the United States or against an opposing military force; or (b) results in the call or order to, or retention on, active duty of members of the uniformed services under Section 688, 12301(a), 12302, 12304, 12304a, 12305, or 12406 of [Title 10], Chapter 15 of [Title 10], Section 712 of Title 14, or any other provision of law during a war or during a national emergency declared by the President or Congress. (Source: Title 10 U.S.C. § 101)

Critical Intelligence Parameter - threat capability or threshold established collaboratively by the requirements sponsor and the capability developer, changes to which could critically impact the effectiveness and survivability of the proposed system. (Source: DIA 5000.200)

Cybersecurity - Prevention of damage to, protection of, and restoration of computers, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (Source: DoD Dictionary of Military and Associated Terms, DoDI 8500.01)

Department of Defense Information Network - The set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. (Source: DoD Dictionary of Military and Associated Terms, JP 6.0)

Defense Business System - Information systems that are operated by, for, or on behalf of the Department of Defense, including financial systems, mixed systems, financial data feeder systems, contracting systems, logistics, planning and budgeting, installations management systems, human resource management systems, and training and readiness systems. A business system does not include a national security system or an information system used

exclusively by and within the defense commissary system or the exchange system or other instrumentality of the DoD conducted for the morale, welfare, and recreation of members of the Armed Forces using non-appropriated funds. (Source: Title 10 U.S.C. § 2222)

Document Sponsor - The organization submitting a capability requirements document. Solution Sponsors for successor documents - CDDs and Joint DCRs - may be different from the Requirement Sponsors for initial documents - ICDs, UONs, JUONs, and JEONs. Different Sponsors for requirements and solutions can occur when the initial document Sponsor does not have acquisition authority and a different organization is designated to develop and field a capability solution, or when one Sponsor elects to leverage a validated document generated by a different Sponsor. (Source: JCIDS Manual)

DoD Components - OSD, the Military Departments, the CJCS, the CCMDs, the Office of the Inspector General of the Department of Defense, the Department of Defense Agencies, Department of Defense field activities, and all other organizational entities in DoD. (Source: DoD Dictionary of Military and Associated Terms)

Family of Systems (FoS) - A set of systems that provide similar capabilities through different approaches to achieve similar or complementary effects For example, the warfighter may need the capability to track moving targets. The FoS that provides this capability could include manned or unmanned aerial vehicles (UAVs) with the appropriate sensors, a space based platform or special operations capability. Each can provide the ability to track moving targets, but with differing characteristics of persistence, accuracy, timeliness, etc. (Source: DoD, 2018, DAU Glossary)

Fielding Targets (IAW Title 10 U.S.C. § 2448a) - the date for initial operational capability (referred to in this section as the "fielding target"). (Source: Title 10 U.S.C. § 2448a)

Gap – See "Capability Gap."

Integrated Priority List (IPL) – A list of a combatant commander's highest priority requirements, prioritized across Service and functional lines, defining shortfalls in key programs that, in the judgment of the combatant commander, adversely affect the capability of the combatant commander's forces to accomplish their assigned mission. Also called IPL. (Source: DoD Dictionary of Military and Associated Terms)

Information Resources - Information and related resources, such as personnel, equipment, funds, and information technology. (Source: Title 44 U.S.C. § 3502)

Information Systems (IS) - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Source: Title 44 U.S.C. § 3502)

Information Technology (IT) -

1. With respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in that automatic acquisition storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the 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 that requires the use - (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product;

2. Includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

3. Does not include any equipment acquired by a federal contractor incidental to a federal contract. (Source: Title 40 U.S.C. § 3502)

Intelligence Interoperability - The ability to receive, produce, store and/or share intelligence data, products, services, and/or processes with similarly compatible systems; and, to render that data, product, service, and/or process to other applicable systems in a readily available format. Intelligence interoperability includes both the technical exchange of information (data) and the operational effectiveness of that exchanged information (service and processes). Intelligence interoperability is more than just information exchange; it includes the harmonization of intelligence systems, processes, procedures, organizations, and missions. (Source: JP 2.0, DoDI 8330.01).

Interoperability -

1. The ability to act together coherently, effectively, and efficiently to achieve tactical, operational, and strategic objectives. (Source: JP 3-0)

2. The condition achieved among communications-electronics systems or items of communications- electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. (Source: JP 6-0)

3. 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 exchanged to enable them to operate effectively together. IT 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 must be balanced with cybersecurity (formerly IA). (Source: DoDI 8330.01)

Joint - Connotes activities, operations, organizations, etc., in which elements of two or more Military Departments participate. (Source: DoD Dictionary of Military and Associated Terms)

Note that this definition of "joint" is applicable to capability requirements documents and capability solutions which apply to more than one DoD Component. See "joint matters" definition derived from Title 10 U.S.C. § 668 and "joint military capability" for the definition applicable to Title 10 U.S.C. § 181 JROC responsibilities.

Joint Concepts - Identifies a current or future military challenge and proposes a solution to improve the ability of the joint force to address that military challenge. A joint concept may also propose new ways to employ the joint force based on future technology. (Source: DoD Dictionary of Military and Associated Terms, CJCSI 3010.02).

Joint Emergent Operational Need (JEON) – UONs that are identified by a CCMD, CJCS, or VCJCS as inherently joint and impacting an anticipated contingency operation. (Source: CJCSI 5123.01)

Joint Matters - In the context of joint matters, the term "integrated forces" refers to military forces that are involved in achieving unified action with participants from more than one military department, or a military department and one or more of the following: other departments and agencies in the United States, the military forces or agencies of other countries, non-governmental persons or entities. (Source: Title 10 U.S.C. § 668)

Joint Military Capabilities - Means the collective capabilities across the joint force, including both joint and force-specific capabilities that are available to conduct military operations. (Source: Title 10 U.S.C. § 181)

Joint Performance Requirement (JPR) - A performance requirement that is critical or essential to ensure interoperability or fulfill a capability gap of more than one armed force, Defense Agency, or other entity of the Department of Defense, or impacts the joint force in other ways such as logistics. (Source: Title 10 U.S.C. § 181)

Joint Urgent Operational Need (JUON) - UONs that are identified by a CCMD, CJCS, or VCJCS as inherently joint and impacting an ongoing contingency operation. (Source: CJCSI 5123.01)

Materiel (Capability Solution) - All items (including ships, tanks, self-propelled weapons, aircraft, etc., and related spares, repair parts, and support equipment, but excluding real property, installations, and utilities) necessary to equip, operate, maintain, and support military activities without distinction as to its application for administrative or combat purposes. See also equipment; personal property. (Source: DoD Dictionary of Military and Associated Terms, JP 4-0)

materiel (Capability Solution) - The letter “m” in the acronym is usually lower case since Joint DCRs do not advocate new materiel development, but rather advocate the identification of materiel items, systems, or equipment needed to support the required capability increased quantities, modifications, improvements, or alternate applications of existing materiel or the purchase of Commercial Off-The-Shelf (COTS), Government Off-The-Shelf (GOTS), or Non-Development Items (NDI). Sometimes referred to as “little m” materiel, the materiel DOTmLPF-P consideration is everything necessary to equip DoD forces to operate effectively. Materiel includes ships, tanks, self-propelled weapons, aircraft, related spares, repair parts, and support equipment, but excludes real property, installations, and utilities.

Mandatory KPPs – These are the Force Protection, System Survivability, Sustainment, and Energy attributes that are designated as mandatory KPPs IAW the applicable provisions of federal law under Title 10 U.S.C.

Mandatory Performance Attributes - These consist of the four mandatory KPPs as well as the Net-Ready Performance Attribute.

Need - See “Capability Requirement.”

Net-Ready - DoD IT that meets required information needs, information timeliness requirements, has a cybersecurity (formerly IA) accreditation, and meets the required attributes to support military operations, to be entered and managed on the network, and to effectively exchange information for both the technical exchange of information and the operational effectiveness of that exchange. DoD IT that is net ready enables warfighters and DoD business operators to exercise control over enterprise information and services through a loosely coupled, distributed infrastructure that leverages service modularity, multimedia connectivity, metadata, and collaboration to provide an environment that promotes unifying actions among all participants. Net readiness requires that IT operate in an environment where there exists a distributed information processing environment in which applications are integrated; applications and data independent of hardware are integrated; information transfer capabilities exist to ensure communications within and across diverse media; information is in a common format with a common meaning; common human-computer interfaces for users and effective means to protect the information exist. Net readiness is critical to achieving the envisioned objective of a cost- effective integrated environment. Achieving and maintaining this vision requires interoperability:

- Within a joint task force or CCMD area of responsibility (AOR).

- Across CCMD AOR boundaries.

- Between strategic and tactical systems.

- Within and across Military Services and agencies.

- From the battlefield to the sustaining base.

- Among U.S., allied, and coalition forces.

- Across current and future systems. (Source: JCIDS Manual)

National Security System - A telecommunications or information system operated by the Federal 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 Is critical to the direct fulfillment of military or intelligence missions.

Limitation. Does not include a system to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (Source: Title 40 U.S.C. § 11103)

Non-materiel (Capability Solution) - Changes to doctrine, organization, training, (fielded) materiel, leadership and education, personnel, facilities, and/or policy, implemented to satisfy one or more capability requirements (or needs) and reduce or eliminate one or more capability gaps, without the need to develop or purchase new materiel capability solutions. (Source: DoD Dictionary of Military and Associated Terms, JP 4-0)

Operational Energy – The energy required for training, moving, and sustaining military forces and weapons platforms for military operations. (Source: DoD Dictionary of Military and Associated Terms)

Performance Attribute – is a characteristic or inherent part of a required system that is needed by the system to achieve satisfactory performance.

Performance Requirement – Consists of performance attributes (KPPs, KSAs, and APAs) of a system that is critical or essential to the development of an effective military capability that does not meet the criteria of a JPR. The Service Chiefs are responsible for all performance requirements for their respective Service. (Source: Title 10 U.S.C. § 181)

Program Costs (IAW Title 10 U.S.C. § 2448a) - The procurement unit cost and sustainment cost (referred to in this section as “program cost targets”).

Requirement - See “Capability Requirement.”

Requirements Definition Package - The RDP (or equivalent) is a first level refinement of one or more capability requirements identified in an IS-ICD or IS-CDD, and is co-developed by the operational user (or representative) and the program office. The RDP (or equivalent) identifies the KPPs, KSAs, and APAs necessary to scope and cost implementation of a capability solution. The RDP (or equivalent) may also identify non-materiel changes that need to be implemented to fully realize the IS capability solution. The RDP (or equivalent) is approved by the delegated oversight authority listed in the IS-ICD or IS-CDD. (Source: JCIDS Manual)

Requirement Sponsor - See “Document Sponsor.”

Solution - See “Capability Solution.”

Solution Sponsor - See “Document Sponsor.”

Sponsor - See “Document Sponsor.”

Spectrum Supportability Risk Assessment (SSRA) - Risk assessment performed by DoD Components for all Spectrum Dependent (S-D) systems to identify risks as early as possible and to affect design and procurement decisions accordingly. These risks are reviewed at acquisition milestones and are managed throughout the system’s lifecycle. (Source: DoD, 2018, DAU Glossary)

System of Systems (SoS) - A set or arrangement that results when independent and useful systems are integrated into a larger system that delivers unique capabilities. SoS may deliver capabilities by combining multiple collaborative and independent-yet-interacting systems. The mix of systems may include existing, partially developed and yet-to-be designed independent systems. (Source: DoD, 2018, DAU Glossary)

Threat - The sum of the potential strengths, capabilities, and strategic objectives of any adversary which can limit or negate mission accomplishment or reduce force, system, or equipment effectiveness. It does not include (a) natural or environmental factors affecting the ability or the system to function or support mission accomplishment, (b) mechanical or component failure affecting mission accomplishment unless caused by adversary action, or (c) program issues related to budgeting, restructuring, or cancellation of a program. (Source: CJCSI 5123.01)

Urgent Capability Acquisitions - A streamlined and tightly integrated iterative approach, acting upon validated urgent or emergent capability requirements, to: conduct analysis and evaluate alternatives and identify preferred solutions; develop and approve acquisition documents; contract using all available statutory and regulatory authorities and waivers and deviations of such, appropriate to the situation; identify and minimize technical development, integration, and manufacturing risks; and rapidly produce and deliver required capabilities. (Source: DoDI 5000.02)

Urgent Operational Need (UON) - Capability requirements identified as impacting an ongoing or anticipated contingency operation. If left unfulfilled, UONs result in capability gaps potentially resulting in loss of life or critical mission failure. When validated by a single DoD Component, these are known as DoD Component UONs. DoD Components, in their own terminology, may use a different name for a UON. (Source: CJCSI 5123.01)

Validation – The review and approval of capability requirements documents by a designated validation authority. The JROC is the ultimate validation authority for capability requirements unless otherwise delegated to a subordinate board or in the case where the independent validation authority is a Service, CCMD, or other DoD Component. (Source: CJCSI 5123.01)