# Joint Publication 3-27

# Homeland Defense


12 July 2007

# PREFACE

## 1. Scope

This publication provides doctrine for the defense of the US homeland across the range of military operations. It provides information on command and control, interagency and multinational coordination, and operations required to defeat external threats to, and aggression against, the homeland.

## 2. Purpose

This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff. It sets forth joint doctrine to govern the activities and performance of the Armed Forces of the United States in operations and provides the doctrinal basis for interagency coordination for defense of the homeland. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders (JFCs) and prescribes joint doctrine for operations and training. It provides military guidance for use by the Armed Forces in preparing their appropriate plans. It is not the intent of this publication to restrict the authority of the JFC from organizing the force and executing the mission in a manner the JFC deems most appropriate to ensure unity of effort in the accomplishment of the overall objective.

## 3. Application

a. Joint doctrine established in this publication applies to the commanders of combatant commands, sub unified commands, joint task forces, subordinate components of these commands, and the Services.

b. The guidance in this publication is authoritative; as such, this doctrine will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise. If conflicts arise between the contents of this publication and the contents of Service publications, this publication will take precedence unless the Chairman of the Joint Chiefs of Staff, normally in coordination with the other members of the Joint Chiefs of Staff, has provided more current and specific guidance. Commanders of forces operating as part of a multinational (alliance or coalition) military command should follow multinational doctrine and procedures ratified by the United States. For doctrine and procedures not ratified by the United States, commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable and consistent with US law, regulations, and doctrine.

For the Chairman of the Joint Chiefs of Staff:

WALTER L. SHARP
Lieutenant General, USA
Director, Joint Staff

Intentionally Blank

# TABLE OF CONTENTS

FIGURE

Intentionally Blank

# EXECUTIVE SUMMARY
## COMMANDER'S OVERVIEW

- **Provides a Thorough Introduction to Homeland Defense Operations**
- **Discusses Command Relationships and Interagency Responsibilities**
- **Describes Air, Land, Maritime, and Space Operations in the Homeland Defense Context**
- **Outlines Other Supporting Homeland Defense Operations and Enabling Activities**

### Introduction

***A secure US homeland is the Nation's first priority.***

Defense of the homeland is the Department of Defense's (DOD's) highest priority with the goal to defeat threats at a safe distance from the homeland.

Homeland defense (HD) is the protection of US sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression, or other threats as directed by the President. DOD is responsible for the HD mission, and therefore leads the HD response, with other departments and agencies in support of DOD efforts.

***Threats.***

In today's complex threat environment, our approach to HD must address all aspects of the operational environment. Externally, the United States has sought to shape the international environment through the application of diplomatic, economic, military, and informational means.

***The number of adversaries that threaten our ability to protect our interests represents a considerable challenge.***

The homeland is confronted by a variety of interrelated threats that demand coordinated procedures and synchronized efforts among US Government (USG) departments and agencies charged with law enforcement and national defense. These threats include any transnational activity including international terrorism, narcotics trafficking, the proliferation of weapons of mass destruction and the delivery systems for such weapons, and organized crime that threatens the national security of the United States. These threats also include extremists and opportunists who enter into relationships of convenience that exploit the capabilities of the other and cloud the distinction between crime and terror.

***Our enemies will continue to employ a variety of tactics that could significantly affect the US economy and global trade.***

Evidence suggests that terrorist organizations have grown more extreme in their objectives and actions and are less concerned that attacks on innocent civilians or public infrastructure will undermine support for their causes. Some groups have attained a considerable degree of financial independence and essentially "declared war" on the United States with little regard as to how we will respond.

***Global Active, Layered Defense.***

The *Strategy for Homeland Defense and Civil Support* calls for securing the United States from attack through an active, layered defense in depth. This active, layered defense seamlessly integrates US capabilities in the forward regions of the world, in the geographic approaches to US territory, and within the US homeland.

***The Homeland Defense (HD) Operational Framework.***

The purpose of HD is to protect against and mitigate the impact of incursions or attacks on sovereign territory, the domestic population, and defense critical infrastructure (DCI). In order to accomplish this, DOD HD objectives are to (1) identify the threat; (2) dissuade adversaries from undertaking programs or conducting actions that could pose a threat to the US homeland; (3) ensure defense of the homeland and deny an adversary's access to the nation's sovereign airspace, territory, and territorial seas; (4) ensure access to space and information; (5) protect DCI; (6) deter aggression and coercion by conducting global operations; (7) decisively defeat any adversary if deterrence fails; and (8) recover from any attack or incident.

HD operations are conducted globally, throughout every operational environment (this includes the air, land, maritime, and space domains and the information environment). While each domain is geographically separate, it is the actions conducted in each of these domains that provide the pillars of HD; together these actions provide the overall HD construct. The information environment is also considered distinct but it resides within each of the four domains. Outside of the United States (in the forward regions and approaches), DOD conducts HD operations to detect, deter, prevent and if necessary defeat adversaries that try to access the homeland. Military activities within the homeland are conducted within the land, airspace, and territorial waters of the United States. These activities require freedom of movement and access to information and space capabilities. Operations may include protection of DCI, air interdiction, maritime interception, land operations, and others.

***HD Legal and Policy Considerations.***

The Constitution provided the basis for HD activities through the guarantee of domestic tranquility and the provision for the common

defense of the Nation. As Commander in Chief, the President must carry out the Constitutional responsibilities of the chief executive, including the protection of the United States from invasion and domestic violence. Guidance to implement this authority comes in many forms to include Presidential directives and orders, laws, court decisions, strategic documents, and policy.

***During the conduct of HD operations, US military forces must be prepared to use force.***

The commitment of military power to resolve crises has traditionally involved the use of lethal weapons or the implicit or explicit threat to use them. However, the nature of HD operations mandates consideration for employment of a variety of weapon capabilities to include those of the nonlethal variety. Self defense is an inherent right and obligation, exercised by the unit commander in response to a hostile act or demonstrated hostile intent. Individual self-defense is exercised IAW establised SROE. Nonlethal capabilities provide an effective alternative means of employing force to reduce the probability of death or serious injury to noncombatants or belligerents. Employment of nonlethal capabilities should be considered for inclusion in HD plans.

***Key Planning Considerations.***

Commanders and their staffs should consider the interrelationship between HD and civil support (CS) operations (i.e., the potential for transition between the mission areas and simultaneous operations) to **address interagency coordination and collaboration in their planning and execution efforts.** Understanding nonmilitary capabilities is key to successful operations. **Capabilities of our multinational partners** are key enablers for DOD planners to consider, particularly for operations in the forward regions and defense of the approaches to the homeland**. Public affairs** (PA) must be included in all phases of planning and coordination from the onset of HD operations. Due to the involvement of other federal agencies in HD missions, military PA will operate in an interagency environment with emphasis on cooperation, coordination, and unity of effort. The goal of PA in HD operations is to ensure all federal agencies speak with one voice and provide consistent, factual information to the public. **Protection** applies domestically in the context of HD. Training and joint intelligence preparation of the operational environment must be conducted to ensure adequate planning and implementation of protection measures. Finally, the Armed Forces of the United States must be prepared to conduct prompt, sustained, and decisive combat operations in **all operating conditions.**

## Command Relationships and Interagency Responsibilities

***Military forces will always remain under the control of the established Title 10, Title 14, or Title 32, US Code chain of command when conducting operations.***

Combatant commanders (CCDRs) exercise combatant command (command authority) of assigned forces, and are directly responsible to the President and the Secretary of Defense (SecDef) for the performance of assigned missions and the preparedness of their commands. CCDRs prescribe the chain of command within their commands and designate the appropriate authority to be exercised by subordinate commanders. **SecDef** has overall authority for DOD and is the President's principal assistant on military matters concerning HD. **Assistant SecDef for Homeland Defense and America's Security Affairs** is responsible for the overall supervision of all DOD HD related activities, including HD and CS missions within DOD. **Assistant SecDef for Special Operations/Low-Intensity Conflict and Interdependent Capabilities** is the principal civilian advisor to SecDef on special operations activities and resources. **Chairman of the Joint Chiefs of Staff** (CJCS) advises the President and SecDef on operational policies, responsibilities, and programs; assisting the SecDef in implementing operational responses to threats or acts of terrorism; and translating SecDef guidance into operation orders. Because their areas of operation include US territory, **Commander, US Northern Command (CDRUSNORTHCOM), Commander, US Pacific Command, (CDRUSPACOM), and Commander, US Southern Command (CDRUSSOUTHCOM)** are the commanders most closely associated with HD activities (they are also referred to in this publication as CCDRs with geographic HD responsibilities). They are responsible for planning, organizing, and executing HD operations within their respective areas of responsibility (AORs). The other CCDRs support them and contribute to the protection of US homeland either through actions within their own AORs or through global responsibilities assigned in the Unified Command Plan. **Commander, US Strategic Command** is responsible for providing the nation with global deterrence capabilities and synchronizing DOD efforts to combat adversary weapons of mass destruction worldwide. For HD, **Commander, US Special Operations Command** serves as a supported or supporting commander for selected counterterrorism activities and serves as a supporting commander to the CCDRs with geographic HD responsibilities within their respective AORs. **Commander, US Transportation Command** provides airlift and tanker forces, as well as base opening and command and control capabilities to supported commanders. **Commander, US Joint Forces Command's** role in HD is to provide support as joint force provider, integrator, and trainer. Finally, **Reserve Component (RC)** forces are integral to the accomplishment of peacetime missions and

conflict prevention. Guidelines for the utilization of RC forces are found in Title 10, United States Code.

***Interagency coordination and interoperability.***

The complex environment in which HD operations are conducted (characterized by an AOR of literally thousands of different jurisdictions, many agencies and organizations, and several allies and coalition partners) necessitates coordinated and integrated operations with our HD partners to ensure the mutual security of our nations, safety of our populations, and viability of our critical infrastructure.

At the strategic level**,** DOD interaction and participation is largely performed by senior DOD and military leaders and their support staff, to include SecDef, Deputy Secretary of Defense, CJCS, and Vice-CJCS in such key committees as the National Security Council, the Homeland Security Council, including their respective Principals Committee and Deputies Committee, and the various policy coordination committees. Operational coordination is conducted within appropriate joint force command centers and their corresponding federal, state, tribal, and local interagency facilities and intergovernmental organizations, nongovernmental organizations, and/or the private sector. Expedited procedures and protocols for coordination of USG defense and security activities are vital to protection of the homeland.

Within the US homeland, DOD and US military forces must effectively deal with time compression of actions, potential impact on US domestic population and DCI, and unique legal and policy guidelines. These forces face continuous media scrutiny, must be sensitive to sovereignty and jurisdictional considerations and mindful of political dimensions of a domestic response, yet responsive enough to deal with the varied threats to the homeland. This environment necessitates an effective interagency process and program.

***Command and control considerations for multinational operations.***

Multinational operations include alliances or coalitions between two or more nations to best achieve their common interests. To conduct the full range of HD operations, the CCDRs with geographic HD responsibilities are required to coordinate actions with all instruments of national power, as well as multinational and nonmilitary organizations.

***Synchronization and integration of HD operations.***

The joint force commander (JFC) must be fully cognizant of the strategic direction in order to establish the priorities, timelines, goals and objectives for HD missions that allow synchronization and integration of air, land, maritime, space and supporting operations for unified action. DOD policies, international and command agreements, federal constitutional and statutory law, security cooperation plans, and selected

operation plans provide guidance which must be integrated by the CCDR to achieve synchronization.

## Air, Land, Maritime, and Space Homeland Defense Operations

***HD air operations.***

DOD is charged with defeating air threats to the United States, such as attacks from military aircraft and ballistic and cruise missiles. DOD must also be prepared to intercept nontraditional threats, even when the intent to harm the United States is uncertain. Early detection and successful interception of these types of potential threats require very close cooperation with DOD's interagency partners.

The combatant commanders with geographic HD responsibilities must consider the unique aspects of aerospace operations within the homeland. Among these unique aspects are the vast areas of operation, the civilian control of airspace, the peacetime environment, the continuous nature of HD operations, and very restrictive engagement criteria.

At the direction of the President through SecDef, DOD conducts homeland air defense using defensive counterair operations, which are comprised of active and passive air and missile defense. Operation Noble Eagle (ONE) is the overall umbrella operation covering HD for North America and Hawaii. As the binational leading element of this operation, NORAD is tasked to support ONE by employing the forces and command and control necessary to protect North America from air attack. Further, because terrorists and other adversaries consider an attack on the National Capital Region (NCR) a continuing goal, it requires focused defense and security measures. DOD employs an integrated air defense system as part of the around-the-clock, multilayered, joint military and interagency, effort. In addition, the Transportation Security Agency and other elements of the Department of Homeland Security, as well as the Department of Justice and the Department of Transportation, conduct significant aviation security efforts throughout the United States and in the NCR. Through the NCR Coordination Center (NCRCC), various agencies have improved situational awareness of the actions of their defense partners. Representatives from other state and local law enforcement agencies and the Joint Air Defense Operations Center also participate at the NCRCC when threats or circumstances warrant.

The likelihood of conventional large-scale land attack on the US may be remote, but the wide-range of threats that do exist must be addressed by land forces conducting HD. Historically, US land forces have

concentrated on defeating threats as far away from the homeland as possible, and that remains the over-arching goal.

***HD land operations.***

Land operations conducted in support of HD require commanders to consider unique elements during planning and execution. More so than during traditional overseas military operations, HD operations also require significant coordination and partnership between federal, state, tribal, and local government and agencies, especially since there is a significant overlap between DOD and law enforcement organization roles and functions.

The CCDRs with geographic HD responsibilities must anticipate, plan, and be prepared for the possibility of land defense operations. Specific defensive land operations in support of HD may include security operations through force protection (FP) tasks or protection of critical defense infrastructure. Offensive operations take the initiative from the enemy, gaining freedom of action creating desired effects to achieve operational objectives. Although land defense forces may be required to defend in the short term, decisive results require shifting to the offense as soon as possible.

As with other military operations, HD operations in the land domain are planned and executed by the CCDRs, through their respective combatant commands, and the subordinate commands; either Service specific task force headquarters, joint task forces, or a joint force land component commander.

***HD maritime operations.***

Securing the maritime domain is essential to keeping the homeland safe. DOD, through the relevant CCDR, is prepared to respond to maritime threats from the forward regions to the homeland. DOD plays the lead role in a maritime HD construct, where DOD is identified as the federal agency with lead responsibility whether it is by discovery of a threat during normal operations, which requires immediate action, or through the protocols established by the Maritime Operational Threat Response (MOTR) Plan.

The MOTR protocols and procedures allow rapid response to short-notice threats and require interagency partners to begin coordination activities at the earliest possible opportunity. The MOTR coordination process is conducted through a virtual network of interagency national and operational command centers. This coordination process is the key element in determining which agency is the right choice for leading the USG response and what other agencies are needed to support the response effort. The goal is to identify threats

as early and as distant from the homeland as possible, but no later than to allow time to defeat or otherwise overcome threats at a safe distance from the United States.

The joint force maritime component commander (JFMCC) plans and executes operations in the maritime domain while supporting the operations of the other components as directed. JFMCC planning must be in consonance with the guidance of senior commanders, must support the JFC concept of operations, and should support other component commanders as well.

Maritime HD operations may be accomplished independently or in support of other operations. When established, a maritime area of operations can include international and territorial waters, harbor approaches, ports, waterfront facilities, and those internal waters and rivers that provide access to port facilities (including associated airspace).

A close alliance of US maritime forces is increasingly crucial to contend with challenges to US sovereignty and maritime HD that continually grow more diverse and complex. Continuous US Navy and US Coast Guard teamwork across the spectrum of maritime operations provides a strong foundation for dealing effectively with emerging challenges that include the global war on terrorism, regional conflict, crisis response, sanctions enforcement, arms trafficking, weapons proliferation, mass migration, smuggling, natural resource depletion, and FP.

Maritime operations in support of HD that require a coordinated government (federal, state, tribal, local) effort range from protection of ports, harbor approach defense, and countermine and mine countermeasures operations to littoral, boarding, and maritime interception operations.

***Space HD operations.***

The region of space above the United States cannot be owned or possessed like territory. It is USG policy, however, that purposeful interference with US space systems will be viewed as an infringement on the Nation's sovereign rights. In order to deter or preempt attacks and protect our military space assets, DOD conducts space operations in support of HD through the space control, space support, space force enhancement, and space force application mission areas.

HD is a high-priority activity, requiring the marshalling of all available space capabilities. Key to maximizing US space capabilities is the successful integration of civilian space assets with military space capabilities. Use of civilian space capabilities is essential to the effectiveness of our ability to successfully accomplish the four space mission areas.

***BMD Operations.*** Ballistic missile defense (BMD) capabilities are designed to detect, deter, defend against and defeat adversary ballistic missile threats. The goal is to build a layered, integrated capability to defeat inbound missiles in all phases of flight and involves passive defense, active defense, attack operations, and battle management. BMD of the homeland includes the synchronization and integration of capabilities to destroy or disrupt adversary missiles in flight or prior to launch. BMD fully synchronizes and integrates offensive and defensive actions and supporting systems to achieve unity of effort. GCCs are responsible for planning and executing ballistic missile defense within their geographic AORs, while CDRUSSTRATCOM is responsible for planning, integrating, coordinating and advocating global missile defense operations and support. BMD employs the operational elements of missile defense to provide protection across the range of operations and has a direct relationship to several other HD (and CS) operations, such as consequence management, DCI, FP, space operations, and combating weapons of mass destruction.

## Other Supporting Operations and Enabling Activities

***The information environment.*** Supporting operations and enabling activities should be considered in the planning and execution of all HD operations. They often overlap with other activities and specific tasks may be closely related. The US conducts operations, including HD, in a complex, interconnected, and increasingly global operational environment. The information environment and activities conducted in each of the domains influence and shape each other.

***Information operations.*** Information operations is the integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.

***Intelligence.*** Knowledge of the enemy is one of the fundamentals of joint warfare. Intelligence is the discipline that provides this knowledge and information about an adversary's capabilities, centers of gravity, and probable

course of action. Intelligence assessments help the commander determine the magnitude of the threat, which forces to deploy, the most efficient manner in which to deploy those forces, and probable enemy reactions.

As part of the overall information environment, the Global Information Grid (GIG) represents the interconnected communications system of DOD. In addition to the DOD GIG, the HD information environment includes non-DOD information infrastructures that can directly support HD operations. DOD requires information from non-DOD organizations and thus, has a reliance on some non-DOD processes, assets, and infrastructures to accomplish the HD mission.

DOD must lead the way in transitioning from a "need to know" to a "need to share" culture. The need to share information is an operational necessity that avoids withholding information and minimizes the potential for operational gaps. The overall goal is to attain seamless access to the trusted information sharing environment for all response forces throughout the AOR.

## CONCLUSION

This publication provides doctrine for the defense of the US homeland across the range of military operations. It provides information on command and control, interagency and multinational coordination, and operations required to defeat external threats to, and aggression against, the homeland. It also includes considerations for transitioning between homeland defense and civil support operations.

# CHAPTER I
# INTRODUCTION

*"This nation must have ready forces that can bring victory to our country, and safety to our people . . . innovative doctrine, strategy, and weaponry . . . to revolutionize the battlefield of the future and to keep the peace by defining war on our terms . . . We will build the security of America by fighting our enemies abroad, and protecting our folks here at home."*

**President George W. Bush**
**10 January 2002 at signing of the**
**2002 National Defense Appropriations Bill**

## 1. General

a. **The Homeland.** A secure US homeland is the Nation's first priority. Defense of the homeland is the Department of Defense's (DOD's) highest priority with the goal to identify and defeat threats at a safe distance from the homeland. The US homeland, described as the physical region that includes the continental United States (CONUS), Alaska, Hawaii, US territories and possessions, and surrounding territorial waters and airspace, is exposed to the possibility of harm from hostile states or non-state actors. The Nation must always be vigilant against such threats. To preserve the freedoms guaranteed by the Constitution, the Nation must have a homeland that is secure from threats and violence, especially terrorism.

b. **Homeland defense (HD) is the protection of US sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression, or other threats as directed by the President.** An "external" threat or aggression is an action, event, or circumstance that originates from outside the boundaries of

*The Nation must have a homeland that is secure from threats and violence, especially terrorism.*

the homeland. Threats planned, prompted, promoted, caused, or executed by external actors may develop or take place inside the boundaries of the homeland. The reference to "external threats" does not limit where or how attacks could be planned and executed. **DOD is responsible for the HD mission, and therefore leads the HD response, with other departments and agencies in support of DOD efforts.** Note that HD differs from homeland security (HS). HS, as defined in the National Strategy for Homeland Security (NSHS), is a concerted national effort to prevent terrorist acts within the United States, reduce America's vulnerabilities to terrorism, and minimize the damage and recover from attacks that do occur. HS missions are those typically conducted by federal, state, tribal, and/or local law enforcement, government agencies, and the private sector and include law enforcement missions related to terrorism and other criminal activities, as well. The distinction between HS and HD is explored further in Appendix A, "Transitioning Between Homeland Defense and Civil Support."

(1) While DOD is the federal agency with lead responsibility for defending against traditional external threats and/or aggression (e.g., nation-state attack), against other threats (e.g., terrorism) DOD may be in support of the Department of Homeland Security (DHS), the Department of Justice (DOJ), or another partner federal agency. DOD support must be properly requested by the agency and then approved by the President or the Secretary of Defense (SecDef). **When ordered to conduct HD operations, DOD coordinates closely with other federal agencies or departments who may be undertaking simultaneous operations to counter the same or other threats.**

(2) HD operations may be conducted in a complex environment characterized by numerous and varied threats, multiple jurisdictions (i.e., federal, state, tribal, and local), nontraditional partners (intergovernmental organizations (IGOs), nongovernmental organizations (NGOs), and private sector), and international partnerships. **This environment makes coordination with interagency and multinational partners imperative to ensure synchronized and integrated operations.** DOD must be prepared to operate in concert with other United States Government (USG) forces that are conducting HS or other law enforcement activities to counter threats to the homeland. This may mean HD operations coincident in time or geography to DHS forces to counter terrorist threats, such as those of a hijacked commercial aircraft or attempts to perpetrate attacks using weapons of mass destruction (WMD) carried on maritime conveyances, among others. The overlap in departmental roles, responsibilities, authorities, and capabilities amongst USG organizations has made the USG review its approach to coordination during operation execution. The approach promotes early identification of the desired USG outcome and subsequent collaboration with operational partners. Guidance such as the Maritime Operational Response (MOTR) Plan, is an example of this new approach to operations.

*Interagency roles, responsibilities, and required coordination protocols for conduct of air defense and maritime security operations to counter threats to the US are contained in the President-approved Aviation Operational Threat Response (AOTR) and MOTR Plans, discussed later in Chapters III and V, respectively. Specific guidance on interagency headquarters planning and command center support of HD operations is found in annex V (Interagency Coordination) of HD concept plans (CONPLANs).*

c. DOD must also engage in emergency preparedness (EP), which consists of measures taken in advance of an emergency to reduce the loss of life and property and to protect a nation's institutions from all types of hazards through a comprehensive emergency management program of preparedness, mitigation, response, and recovery. EP is considered a part of DOD's overall preparedness activities. **EP is not a stand-alone activity, but an integral part of training, mitigation, and response for both HD and civil support (CS)**.

d. DOD's other mission in securing the homeland is CS, which is conducted in support of other federal, state, tribal and/or local authorities when requested, and approved by the President or SecDef. HD and CS missions may occur simultaneously and require extensive coordination, integration, and synchronization. In addition, HD operations may transition to or from CS. Considerations regarding transition operations are covered in more detail, in Appendix A, "Transitioning between Homeland Defense and Civil Support."

*For more information on CS, see Joint Publication (JP) 3-28*, Civil Support.

## 2. Threats

In today's complex threat environment, **our approach to HD must address all aspects of the operational environment.** Externally, the United States has sought to shape the international environment through the application of diplomatic, economic, military, and informational means. Given the persistent nature of current threats, a proactive, comprehensive approach to HD is required. The uncertainty of the strategic environment is influenced by numerous factors (see Figure I-1).

a. The homeland is confronted by a variety of interrelated threats that demand coordinated procedures and synchronized efforts among USG departments and agencies charged with law enforcement and national defense, particularly those that have overlapping roles, responsibilities, authorities, and capabilities. These include transnational threats – defined in Title 50, United States Code (USC), Section 402 as "any transnational activity (including international terrorism, narcotics trafficking, the proliferation of weapons of mass destruction and the delivery systems for such weapons, and organized crime) that threatens the national security of the United States." These threats also include extremists (e.g., foreign terrorist organizations) and opportunists (e.g., drug cartels and alien smuggling organizations) who enter into relationships of convenience that exploit the capabilities of the other and cloud the distinction between crime and terror.

b. Other threats originate from an adversary's choice of weapons that ranges from nonlethal to lethal capabilities (e.g., conventional, psychological, informational, chemical, biological, radiological, nuclear and high-yield explosives [CBRNE] weapons). Weapons and tactics designed to kill or terrorize large numbers of people or destroy facilities of strategic importance are within the capabilities of many of our adversaries.


**Figure I-1. Homeland Defense Strategic Threat Environment**

c. Adversaries have or are obtaining WMD and the means to deliver them, including long-range ballistic missiles. The terrorist attacks of September 11, 2001 illustrate an adversary's capabilities and willingness to use asymmetric approaches. **Successfully countering symmetric and asymmetric threats and reducing risks requires a concerted and coordinated effort by DOD and other federal agencies; state, tribal, and local governments; and every citizen.**

d. A complex, uncertain, and volatile threat environment presents the United States with a resource-intensive challenge at home and abroad. The number of adversaries that threaten our ability to protect our interests represents a considerable challenge. Our world appears smaller today because of the range, speed, and capability of modern weapons and the ease with which information can be made available. Today, technology and access to information present new challenges in an increasingly global economy. A number of regional powers, non-state actors, and transnational groups possess the capability to challenge the interests of the United States and those of our allies. Adversaries have taken advantage of this technology and employ it in their own operations, in areas such as moving money, communicating with cells in their organizations, approving missions, or conducting intelligence, surveillance, and reconnaissance on potential targets. They are also using these advances, especially in information technology and media, to wage propaganda campaigns and various forms of information operations (IO) against the United States and our allies. In spite of intensive counterproliferation and arms control efforts, the likelihood that adversaries will employ WMD against the United States or its interests has increased. A

CBRNE attack could come in a variety of forms, from release through conventional means such as a ballistic missile to unconventional means (e.g., a "suitcase" radiological device).

e. **Risk remains from terrorist (state and non-state sponsored) and traditional nation-state attacks.** Among these, terrorist and extremist groups and their networks currently pose the greatest nontraditional threat and they remain determined to strike the US homeland. Evidence suggests that terrorist organizations have grown more extreme in their objectives and actions and are less concerned that attacks on innocent civilians or public infrastructure will undermine support for their causes. Some groups have attained a considerable degree of financial independence and have essentially "declared war" on the United States with little regard as to how we will respond. Regardless of source, our enemies will continue to employ a variety of tactics, in particular asymmetric employment of weapons, platforms, and information that could significantly affect the US economy and global trade.

*See JP 3-07.2,* Antiterrorism, *for more information on countering terrorist threats.*

f. **There is a persistent threat to our homeland posed by the influx of illegal immigrants, special interest aliens, drugs, and contraband.** Criminal organizations have established networks to move people, drugs, or other contraband; although these networks have been used for illegal immigrants seeking work, they can also be used for terrorists who want to conduct violent acts. While only in unique and/or extraordinary circumstances would DOD take the lead to secure our borders, transnational threats pose a serious danger to the Nation and require the combined efforts of law enforcement agencies (LEAs), intelligence agencies, and support from DOD assets to enhance LEA efforts to secure our borders and conduct counter illicit trafficking operations.

*See JP 3-07.4,* Joint Counterdrug Operations *and JP 3-28,* Civil Support.

### 3. Global Active, Layered Defense

a. The *Strategy for Homeland Defense and Civil Support* calls for securing the United States from attack through an active, layered defense in depth. This active layered defense seamlessly integrates US capabilities in the forward regions of the world, in the geographic approaches to US territory, and within the US homeland.

b. **The Forward Regions**. The forward regions are foreign land areas, sovereign airspace, and sovereign waters outside the homeland. In the forward regions, the objective is to detect, deter, prevent, or when necessary, defeat threats to the United States. Actions span the range of military operations and may include combat operations, engagement activities, peace operations, or preemptive measures such as direct action missions, computer network attack and defense or global strikes.

c. **The Approaches**. The approaches extend from the limits of the homeland to the forward regions. The approaches are not uniformly defined, may not have boundaries and may be characterized based on a specific situation. The primary objective of actions within the approaches is to locate threats as far from the homeland as possible and defeat them at a

safe distance. These actions conducted in the approaches to counter threats may span the range of USG operations. The National Military Strategy (NMS) emphasizes the importance of joining the efforts of multinational partners and other USG agencies to form an integrated defense of the air, land, maritime, and space approaches to US sovereign territory. Protecting these approaches requires enhanced, persistent surveillance that allows the United States to detect, track, and if required, interdict and defeat potential threats.

d. **The Homeland.** The US homeland includes CONUS, Alaska, Hawaii, US territories and possessions, and the surrounding territorial waters and airspace. In the event that defeating threats in forward regions and approaches fail, DOD must be postured to take immediate, decisive action to defend against and defeat the threat in the homeland. Actions in the homeland may take place simultaneously and in coordination with operations conducted in the approaches and/or forward regions.

## 4. The Homeland Defense Operational Framework

a. The purpose of HD is to protect against and mitigate the impact of incursions or attacks on sovereign territory, the domestic population, and defense critical infrastructure (DCI). The following are DOD HD objectives:

(1) Identify the threat.

(2) Dissuade adversaries from undertaking programs or conducting actions that could pose a threat to the US homeland.

(3) Ensure defense of the homeland and deny an adversary's access to the nation's sovereign airspace, territory, and territorial seas.

(4) Ensure access to space and information.

(5) Protect DCI.

(6) Deter aggression and coercion by conducting global operations.

(7) Decisively defeat any adversary if deterrence fails.

(8) Recover from any attack or incident.

b. The diversity of threats requires that the military instrument of national power take a broad role in **preparing for, detecting, deterring, preventing, defending against, and defeating threats**. It also has a broad role in supporting **recovery** from attacks. HD operations fall within this overarching framework and must be synchronized to ensure success. This requires coordination of activities across time, space, and purpose, as well as interagency coordination and coordination with IGOs, NGOs, and the private sector to defend the homeland.

c. **HD operations are conducted globally, throughout every operational environment (this includes the air, land, maritime, and space domains and the information environment).** While each domain is geographically separate, it is the actions conducted in each of these domains that provide the pillars of HD; together these actions provide the overall HD construct. The information environment is also considered distinct but it resides within each of the four domains. HD operations are conducted in accordance with the law; treaties and international agreements; national authorities; and DOD, Chairman of the Joint Chiefs of Staff (CJCS), joint, military department, and military Service policy, directives, and doctrine. DOD conducts offensive and defensive actions (to include preemptive activities) in order to deter, disrupt, and destroy adversary capabilities at their source. HD operations may be active or passive. Figure I-2 illustrates these relationships.

(1) Outside of the United States (in the forward regions and approaches), DOD conducts HD operations to detect, deter, prevent, and, if necessary, defeat adversaries that try to access the homeland. Activities include maintaining our freedom to operate in space, access information, and conduct campaigns or operations to disrupt and defeat terrorists and other adversaries before they are able to launch an attack within the US homeland. Finally, DOD security cooperation initiatives (e.g., exercises, exchanges, experimentation, and counterproliferation and nonproliferation activities) foster positive working relationships and interoperability with friends and allies.

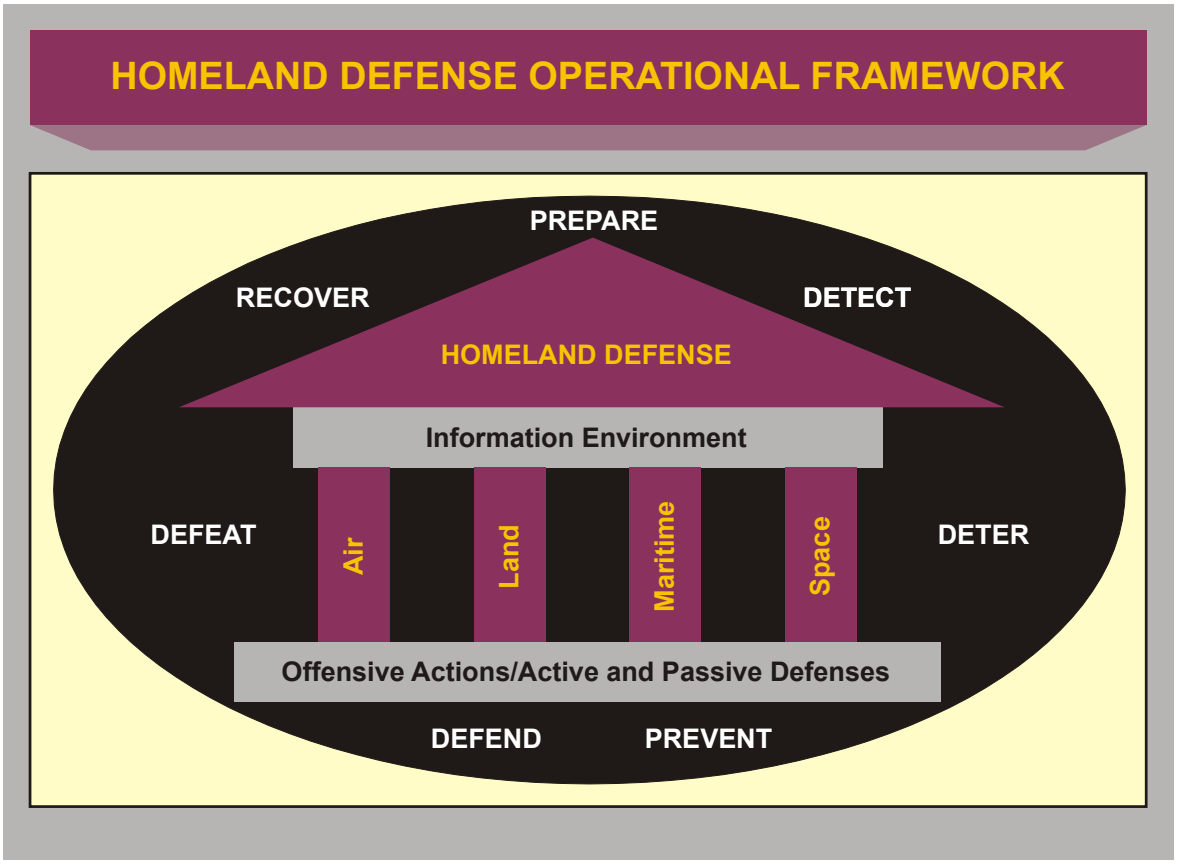



**Figure I-2. Homeland Defense Operational Framework**

(2) Military activities within the homeland are conducted within the land, airspace, and territorial waters of the United States. These activities require freedom of movement and access to information and space capabilities. Operations may include protection of DCI, air interdiction, maritime interception, land operations, and others.

d. **HD operations begin with thorough preparation.** HD EP activities are undertaken to ensure DOD processes, procedures, and resources are in place to support the President and SecDef in designated national security emergencies. DOD EP activities at the strategic level may focus on actions associated with continuity of government (COG) and continuity of operations (COOP). However, at the operational level, DOD emergency preparations to defend the homeland include activities such as joint and interagency interoperability and coordination preparation, joint training exercises and experimentation, and development of information and intelligence architectures.

e. **Early detection is imperative in facilitating timely response to and decisively engaging threats before they reach the homeland**. In the forward regions and approaches persistent intelligence, surveillance, and reconnaissance (ISR) provides decision makers with early warning and assessments. For the CONUS portion of the air domain, this is integrated with North American Aerospace Defense Command's (NORAD's) tactical warning/attack assessments. The United States and its multinational partners seek a global awareness of all threats to our national security individually and collectively to increase our ability to deal with threats at home and abroad.

f. **Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction or the prospect of mission failure.** Deterring adversaries is a key HD objective. DOD EP activities, coupled with offensive and defensive capabilities, may deter an adversary from threatening or attacking the homeland. Well-trained, rapidly deployable forces conducting realistic exercises provide another example of actions and capabilities that may serve as a deterrent.

g. **Prevention of attacks on the homeland** includes security procedures undertaken by the public and private sectors in order to discourage terrorist acts. The United States and its multinational partners work together to synchronize activities, which may also include diplomatic, economic, and political measures.

h. If deterrence and prevention fails, **DOD must be prepared to rapidly respond by defending against threats and aggression**. DOD, as directed by the President, may conduct preemptive and/or offensive HD actions in accordance with international and domestic law, national policy, and directives. The objective of these operations is to destroy, degrade, disrupt, or neutralize weapons, launch platforms, supporting command, control, and communications, logistics and ISR capabilities before they are employed by an adversary. Air, land, maritime, space, and special operations forces (SOF) may conduct offensive actions. Examples of offensive operations may include global strikes. Global strikes may be described as rapidly planned, limited-duration, extended-range precision attacks that are conducted to achieve strategic objectives. They may be executed against

highly valued adversary assets using lethal and nonlethal methods. Targets include adversary centers of gravity; WMD, their delivery systems, production facilities, and storage sites; key leadership; and critical infrastructure. Other examples of HD offensive actions include direct action, space denial, and computer network attack.

i. **Primary defensive actions** associated with HD missions include active and passive defense measures to defeat threats that are already deployed or en route to the target. Active defenses employ limited offensive action and counterattacks to deny a contested area or position to the enemy and are designed to reduce the effectiveness of or stop attacks on our sovereign territory, domestic population, and DCI. Active defenses employ air, land, maritime, space, and SOF. Defenses may also include IO capabilities to disrupt adversary information systems. The objective of HD passive defense is to reduce the probability of, and minimize the damage caused by, hostile actions. Passive defenses include force protection (FP) and critical infrastructure risk mitigation actions to reduce targeting effectiveness. They are normally developed and executed throughout the defending force. Passive defense measures include selected FP actions, deception, mobility, dispersion, systems hardening and protective construction, strategic, operational, and tactical warning and surveillance, and operations security (OPSEC).

j. **Recovery actions** from an HD perspective are those actions taken by a military force during or after operational employment to restore its combat capability to its full operational readiness.

k. **Information Environment**. The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. The actors include leaders, decision makers, individuals, and organizations. Resources include the materials and systems employed to collect, analyze, apply, or disseminate information. The information environment is where humans and automated systems observe, orient, decide, and act upon information, and is therefore the principal environment of decision making. Even though the information environment is considered distinct, it resides within each of the four domains of air, land, maritime, and space. The information environment is made up of three interrelated dimensions: physical, informational, and cognitive. More on the information environment is provided in Chapter VII, "Other Supporting Operations and Enabling Activities."

## 5. Homeland Defense Legal and Policy Considerations

a. There are a variety of documents that provide guidance for conducting HD operations. Figure I-3 lists a number of the key documents that assist military forces in planning and conducting HD missions. Specific planning factors, requirements, and objectives for HD operations are contained in operation plans (OPLANs) and CONPLANs associated with the HD mission. An additional list of documents that provide guidance for the HD mission is included in Appendix D, "Key Homeland Defense Legal and Policy Documents."

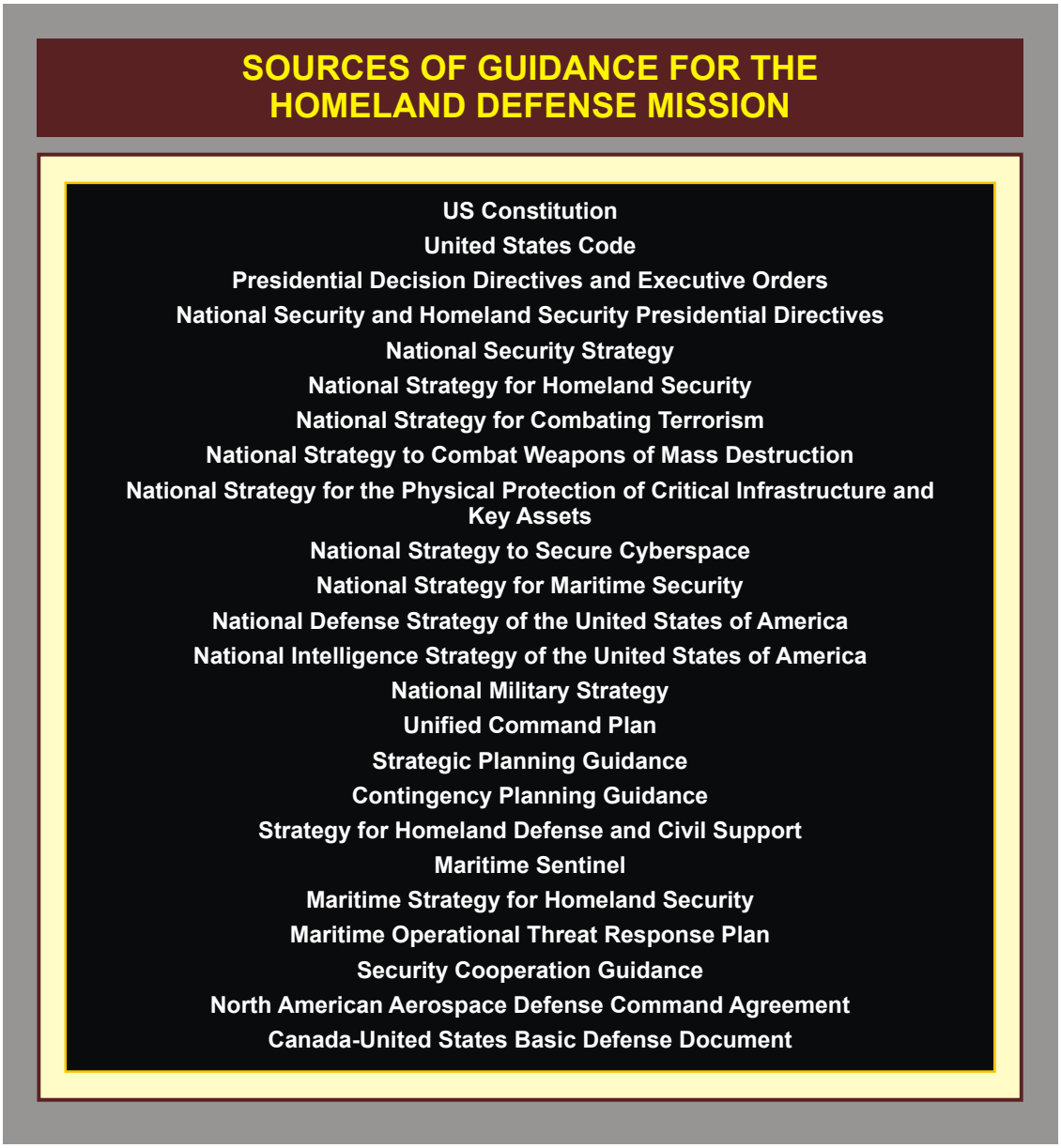



**Figure I-3. Sources of Guidance for the Homeland Defense Mission**

b. **Basic Principles. The Constitution provides the basis for HD activities** through the guarantee of domestic tranquility and the provision for the common defense of the Nation. Under Article II of the US Constitution, the President is given the authority as the Commander in Chief of the Armed Forces and of the militia of several states when called into the actual service of the United States. As Commander in Chief, the President must carry out the Constitutional responsibilities of the chief executive. Article IV, Section 4 of the Constitution also requires the "United States" to protect the states from invasion and domestic violence. This includes the authority of the President as the Commander in Chief. Guidance comes in many forms to include Presidential directives and orders, laws, court decisions, strategic documents, and policy.

c. **Special Considerations.** Certain functions, such as intelligence operations, rules of engagement (ROE), and rules for the use of force (RUF), have specific applications and legal implications when conducted domestically.

(1) **Intelligence Activities.** Intelligence activities refer to all activities that DOD intelligence components are authorized to undertake in accordance with (IAW) DOD Directive (DODD) 5240.1, *DOD Intelligence Activities*. Intelligence activities include the collection, production, and dissemination of foreign intelligence and counterintelligence by DOD intelligence components. Counterintelligence is information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorist activities. IAW DODD 5240.1, *DOD Intelligence Activities*, foreign intelligence is information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence except for information on international terrorist activities.

(a) Intelligence activities conducted by US intelligence organizations in the United States and its territories are strictly controlled. There are several regulations and laws that specifically govern the use of DOD intelligence assets and organizations in domestic operations. The program that covers the collection of information on US persons by the intelligence organizations is called intelligence oversight. Intelligence oversight ensures that intelligence personnel shall not collect, retain, or disseminate information about US persons unless done in accordance with specific guidelines. At the same time, intelligence oversight allows US intelligence organizations to obtain intelligence information required to protect our national security. Figure I-4 lists several policy and guidance documents for the intelligence oversight program. The guidance includes details on program implementation.

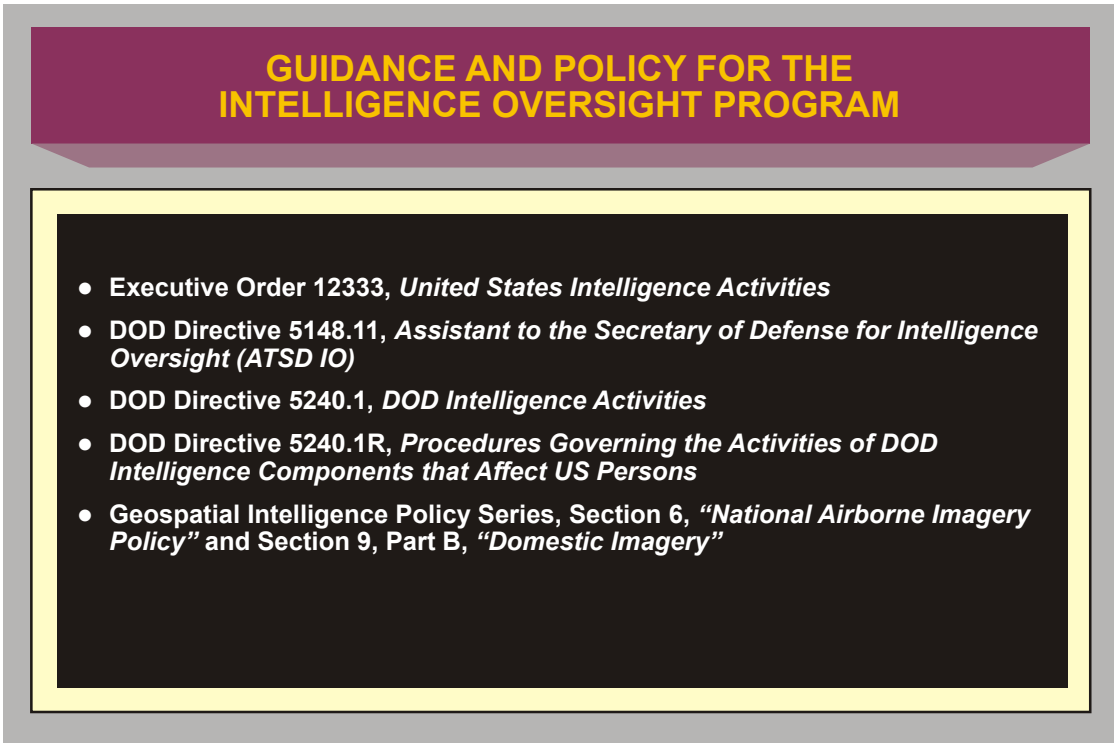



**Figure I-4. Guidance and Policy for the Intelligence Oversight Program**

(b) Publicly available open source information can be used to obtain basic situational awareness and regional industrial knowledge on any part of the world; however, intelligence oversight still applies to information gathered on US persons or companies. Open source information can enhance a commander's awareness of the operational environment.

(c) **Acquisition of Information Concerning Persons and Organizations Not Affiliated with DOD.** Some restrictions on information gathering apply DOD wide. IAW DODD 5200.27, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense,* DOD policy prohibits collecting, reporting, processing, or storing information on individuals or organizations not affiliated with DOD except in those limited circumstances where such information is essential to the accomplishment of certain DOD missions outlined within the directive. Exceptions are defined in DODD 5240.1, *DOD Intelligence Activities*.

*Details on intelligence support to HD can be found in Chapter VII, "Other Supporting Operations and Enabling Activities," and JP 2-0,* Joint Intelligence.

(2) **Psychological Operations.** Under law, psychological operations (PSYOP) will not be conducted against US persons. However, PSYOP personnel and equipment may be used to support approved HD public affairs (PA) activities such as information dissemination, printing, reproduction, distribution, and broadcasting.

*A more complete discussion can be found in JP 3-53,* Doctrine for Joint Psychological Operations.

(3) **Rules of Engagement and Rules for the Use of Force**. During the conduct of HD operations, US military forces must be prepared to use force. The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3121.01B, *Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces* establishes fundamental policies and procedures governing the actions to be taken by US military commanders and personnel during global DOD operations including HD operations.

(a) ROE are directives issued by competent military authorities delineating the circumstances and limitations under which US forces will initiate or continue operations. The standing ROE (SROE) establish fundamental policies and procedures governing the action to be taken by US commanders during all military operations, contingencies and routine military functions occurring outside US territory for mission accomplishment and the exercise of self-defense. **SROE also apply to air and maritime HD missions conducted within US territory or territorial seas, unless otherwise directed by SecDef**. **SROE do not apply to law enforcement and security duties on DOD installations and off-installation while conducting official DOD security functions.** Supplemental ROE may be necessary to meet mission-specific ROE requirements.

(b) RUF are directives issued to guide US forces on the use of force during various operations. The standing RUF (SRUF) apply to land HD missions occurring within

US territory and to DOD forces, civilians, and contractors performing law enforcement and security duties at all DOD installations within or outside US territory, unless otherwise directed by SecDef. Geographic combatant commanders (GCCs) may augment SRUF by submitting a request for mission-specific RUF to CJCS for SecDef approval.

(c) ROE and RUF must conform to appropriate laws including federal law, the law of war, other relevant international law, and military law and they must conform to the situation and locality involved. In cases where National Guard (NG) forces are under state control, state ROE will apply. **Commanders must educate their personnel on ROE and RUF and train them on the use of lethal and nonlethal force**. Self-defense is an inherent right and obligation exercised by the unit commander in response to a hostile act or demonstrated hostile intent. Individual self-defense is exercised IAW established SROE.

(d) Employment of Fires. The commitment of military power to resolve crises has traditionally involved the use of lethal weapons or the implicit or explicit threat to use them. However, the nature of HD operations mandates consideration for employment of a variety of weapon capabilities to include those of the nonlethal variety. Nonlethal capabilities may provide an effective alternative means of employing force to reduce the probability of death or serious injury to noncombatants or belligerents. **Employment of nonlethal capabilities should be considered for inclusion in HD plans, ROE, and RUF**. Additionally, commanders should plan for and conduct ROE and/or RUF rehearsals to prepare their personnel for operations in defense of the homeland.

*Additional information on the employment of nonlethal capabilities can be found in multi-Service publication Field Manual (FM) 3-22.40, Marine Corps Warfighting Publication (MCWP) 3-15.8, Navy Tactics, Techniques, and Procedures (NTTP) 3-07.3.2, Air Force Tactics, Techniques and Procedures (AFTTP) 3-2.45 and US Coast Guard Publication 3-07.31,* NLW – Tactical Employment of Nonlethal Weapons.

## 6. Key Planning Considerations for Homeland Defense Operations

a. **Interagency Coordination**. Within the context of DOD involvement, interagency coordination is that which occurs between elements of DOD and engaged USG agencies for the purpose of achieving an objective. It forges a vital link between the instruments of national power and other jurisdictional entities. DOD conducts interagency coordination at the strategic, operational, and tactical levels through mutual sharing of situational awareness and participation in planning, training, exercises, education, and operations. **Commanders and their staffs should consider the interrelationship between HD and CS operations (i.e., the potential for transition between the missions and simultaneous operations) to address interagency coordination and collaboration in their planning and execution efforts.** Understanding nonmilitary capabilities is key to successful operations.

b. **Multinational Coordination**. The need to collaboratively develop operation plans extends to our allies and coalition partners. **Capabilities of our multinational partners** are key enablers for DOD planners to consider, particularly for operations in the forward regions and defense of the approaches to the homeland.

*For more detailed information on interagency and multinational coordination see JP 3-08*, Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations, *and JP 3-16*, Multinational Operations.

c. **Public Affairs**. The role of PA in HD operations is to support the joint force commander (JFC) by communicating truthful and factual unclassified information about DOD activities to US, allied, national, international, and internal audiences. Due to the involvement of other federal agencies in HD missions, military PA will operate in an interagency environment with emphasis on cooperation, coordination, and unity of effort. The goal of PA in HD operations is to ensure all federal agencies speak with one voice and provide consistent, factual information to the public. The federal agency with lead responsibility develops the key messages and provides PA guidance. Supporting agencies conduct their respective PA operations in concert with this guidance. PA must be included in all phases of planning and coordination from the onset of HD operations.

*For more information on PA, see JP 3-61,* Public Affairs.

d. **Protection.** The protection function focuses on conserving the joint force's fighting potential in four primary ways — **active defensive** measures that protect the joint force, its information, its bases, necessary infrastructure, and lines of communications from an adversary's attack; **passive defensive** measures that make friendly forces, systems, and facilities difficult to locate, strike, and destroy; applying technology and procedures to reduce the risk of fratricide; and **emergency management and response** to reduce the loss of personnel and capabilities due to accidents. It includes, but extends beyond, FP to encompass protection of US noncombatants; the forces, systems, and civil infrastructure of friendly nations; and other government agencies, IGOs and NGOs. The protection function applies domestically in the context of HD.

(1) There are protection considerations that affect planning in every joint operation. Even in a permissive environment risks exist from terrorism, criminal enterprises, environmental threats/hazards, and computer hackers. **Training and joint intelligence preparation of the operational environment must be conducted to ensure adequate planning and implementation of protection measures**.

(2) GCCs are responsible for implementing an antiterrorism (AT) program in their areas of responsibility (AORs). The AT program is designed to prevent and detect terrorist attacks against DOD personnel, their families, facilities, resources, installations, and DCI, as well as the preparation to defend against, and plan the response to, the consequences of terrorist incidents.

(3) FP includes actions taken to prevent or mitigate hostile actions against DOD personnel (to include family members), resources, facilities, and critical information. It does not include actions to defeat the enemy or protect against accidents, weather, or disease. All GCCs have FP responsibilities for their respective AORs to include those who's AORs contain geographic areas of the homeland. Force health protection (FHP) compliments FP

and includes all measures to provide for the health and safety of Service members (Chapter VII provides more information on FHP).

(4) Tactical control (TACON) for DOD FP provides directive authority and control for FP to a GCC; however, it does not necessarily provide TACON for non-FP missions. It allows the GCCs to change, modify, prescribe, and enforce FP conditions (of which AT measures are integral) for covered individuals. Commander, US Northern Command (CDRUSNORTHCOM) has overall DOD AT program and FP responsibility in CONUS. However, CDRUSNORTHCOM's TACON for FP authority does not apply to DOD family members. Day-to-day execution of the FP mission is accomplished by the Services, the DOD agencies, DOD field activities headquarters, and the combatant command headquarters located in the US Northern Command (USNORTHCOM) AOR. USNORTHCOM's AT program and FP measures are outlined in the *USNORTHCOM Antiterrorism (AT) Operations Order*.

*For a complete description of the protection function and its elements, see JP 3-0,* Joint Operations. *For more information on DOD AT and FP programs, refer to DODD 2000.12*, DOD Antiterrorism Program, *Department of Defense Instruction (DODI) 2000.16*, DOD Antiterrorism Standards, *and JP 3-07.2*, Antiterrorism.

e. **Hazardous Operating Environments**. The Armed Forces of the United States must be prepared to conduct prompt, sustained, and decisive combat operations in all operating conditions. This includes conditions resulting from deliberate or inadvertent use of CBRNE, man-made and accidental release of toxic industrial materials; and naturally occurring biological events such as pandemic diseases. Commanders and their staffs must take these potential conditions into account during planning and execution; ensuring that they plan, train, and exercise with their interagency counterparts in preparation for HD operations in any environment.

*Detailed information on conducting military operations in contaminated environments is found in JP 3-11*, Joint Doctrine for Operations in Nuclear, Biological, and Chemical Environments *and JP 3-40,* Joint Doctrine for Combating Weapons of Mass Destruction.

Intentionally Blank

# CHAPTER II
# COMMAND RELATIONSHIPS AND INTERAGENCY RESPONSIBILITIES

*"In uniform, when I talk about terrorism it's easy to assume that the war on terrorism is a military thing. It's not at all. It demands the attention and action of all [sic. instruments] of national power."*

**Gen. Richard B. Myers**
**Chairman of the Joint Chiefs of Staff**
**1 October 2001 – 30 September 2005**

## 1. General

a. For the HD mission, the President, exercising his constitutional authority as Commander in Chief, authorizes military action to counter threats to and within the United States. For the accomplishment of the HD mission, DOD conducts operations globally, throughout every operational environment.

b. Combatant commanders (CCDRs) exercise combatant command (command authority) (COCOM) of assigned forces, and are directly responsible to the President and SecDef for the performance of assigned missions and the preparedness of their commands (Figure II-1 depicts the GCCs' AORs). CCDRs prescribe the chain of command within their commands and designate the appropriate authority to be exercised by subordinate commanders.

*For detailed discussion of command relationships, see JP 1,* Doctrine for the Armed Forces of the United States *and Section II,* Forces for Unified Commands Memorandum.

## 2. Command and Control Relationships and Responsibilities

a. Military forces will always remain under the control of the established Title 10 USC, Title 14 USC, or Title 32 USC chain of command when conducting operations.

(1) **SecDef.** As the President's principal assistant on military matters, the SecDef has overall authority for DOD, hence the conduct and execution of the HD mission resides with SecDef.

(2) **Assistant SecDef for Homeland Defense and America's Security Affairs (ASD[HD&ASA]).** ASD(HD&ASA) is within the office of the Under Secretary of Defense for Policy (USD[P]). ASD(HD&ASA) is responsible for the overall supervision of all DOD HD related activities. The principal duty of ASD(HD&ASA) is to provide overall supervision of the HD and CS missions within DOD. For HD, ASD(HD&ASA) serves as the principal staff assistant and advisor to SecDef, the USD(P) and Deputy Secretary of Defense for matters including, but not limited to the following:

(a) Preparedness to execute the national security missions of DOD pertaining to the HD of US sovereignty, territory, domestic population, and DCI.

(b) Defense Critical Infrastructure Program (DCIP).

(c) DOD domestic AT in accordance with DOD Directive 2000.12, *DOD Antiterrorism (AT) Program*.

(d) DOD domestic counterterrorism (CT) activities, except those executed by SOF.

(e) DOD continuity-related activities, to include COOP, COG, and enduring constitutional government managed under the Defense Continuity Program.

(f) Policy guidance on HD-related education, training, and professional development programs.

*See JP 3-28,* Civil Support*, for specifics on CS operations.*

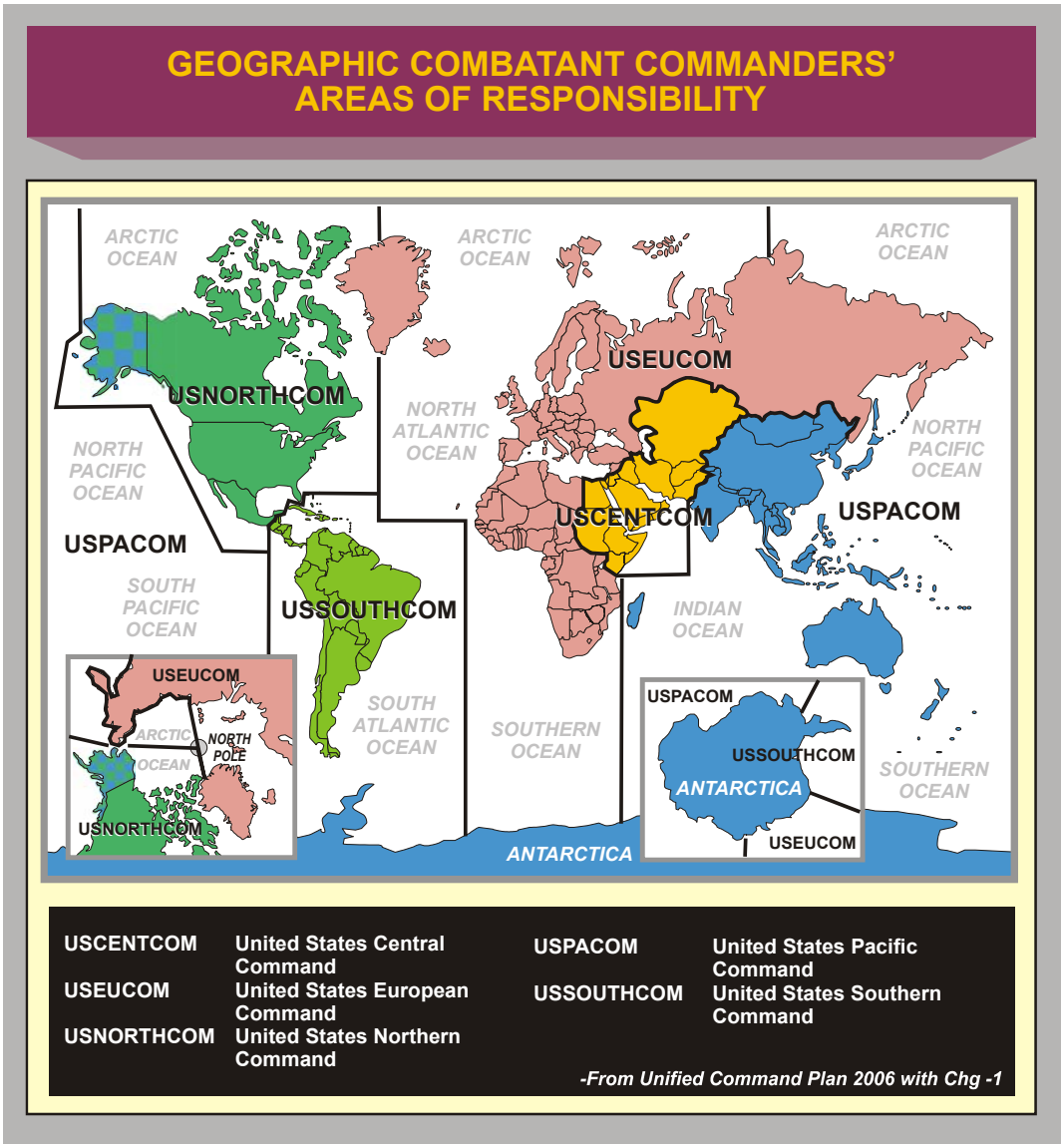



**Figure II-1. Geographic Combatant Commanders' Areas of Responsibility**

(3) **Assistant SecDef for Special Operations/Low-Intensity Conflict and Interdependent Capabilities (ASD[SO/LIC&IC]).** ASD(SO/LIC&IC), under the USD(P), is the principal civilian advisor to SecDef and USD(P) on special operations/low-intensity conflict activities of DOD. This includes development and oversight of implementation of policy for DOD special operations (SO) activities and resources.

(4) **Assistant to the SecDef for Nuclear and Chemical and Biological Defense Programs (ATSD[NCB]).** ATSD(NCB) is directly responsible to SecDef for matters associated with nuclear weapons safety and security, chemical weapons demilitarization, and chemical and biological defense programs.

(5) **Assistant SecDef for Health Affairs (ASD[HA]).** The ASD(HA) is the principal staff assistant and advisor to the Secretary and Deputy Secretary of Defense and the Under Secretary of Defense for Personnel and Readiness for all DOD health policies, programs, and activities. The ASD (HA) has the responsibility to effectively execute DOD's healthcare mission to maintain readiness and to provide healthcare services and support to members of the Armed Forces during military operations. In addition, DOD is a critical component in the Services activation of the federal coordinating centers that locate all civilian beds in a geographic location, arrange the transport of patients from arriving aircraft, and are responsible for all logistics of receiving mass casualties from a disaster area.

(6) **Assistant SecDef for Reserve Affairs (ASD[RA]).** ASD(RA) is responsible for monitoring Reserve Component (RC) readiness and provides policy regarding the appropriate integration of RC forces into HD efforts.

(7) **Chairman of the Joint Chiefs of Staff.** As principal military advisor to the President and the SecDef, the CJCS has numerous responsibilities relating to HD and CS. These include advising the President and SecDef on operational policies, responsibilities, and programs; assisting SecDef in implementing operational responses to threats or acts of terrorism; and translating SecDef guidance into operation orders. The CJCS ensures that HD plans and operations are compatible with other military plans and assists CCDRs in meeting their operational requirements for executing HD operations that have been approved by SecDef.

*See JP 3-28,* Civil Support *for additional information.*

b. **Commander, NORAD and Geographic Combatant Commander Responsibilities**. The Unified Command Plan (UCP) establishes the combatant commands' missions, responsibilities, geographic AORs, and functions. As stipulated in the UCP, the GCCs of USNORTHCOM, US Pacific Command (USPACOM), and US Southern Command (USOUTHCOM) have specified tasks for HD activities (these commanders are referred to subsequently in this publication as CCDRs with geographic HD responsibilities). They are responsible for planning, organizing, and executing HD operations within their respective AORs. The other CCDRs support them and contribute to the protection of the US homeland either through actions within their own AORs (forward regions and approaches) or through global responsibilities assigned in the UCP.

(1) **Commander, North American Aerospace Defense Command (CDRNORAD)**. By international agreement CDRNORAD leads the binational command composed of Canadian and US forces. NORAD's primary missions are: aerospace warning, aerospace control, and maritime warning for North America. CDRNORAD is responsible to the Canadian and US governments through the Chief of Defence Staff (CDS) and CJCS, respectively. CDRUSNORTHCOM is responsible to SecDef. While NORAD and USNORTHCOM have separate missions defined by separate sources, parts of the USNORTHCOM AOR overlaps with NORAD's operational area (OA) (note that in the NORAD Agreement this is normally referred to as an area of operations "AO"). The organizations are separate commands, and neither is subordinate to the other or a part of the other, but their operational focus runs parallel in detecting, tracking, deterring, and if necessary, defeating threats in the air approaches and airspace of North America. NORAD and USNORTHCOM also share in the maritime warning mission. See Appendix C, "North American Aerospace Defense Command, Missions, Organization, and Structure" for detailed information on NORAD.

(2) **CDRUSNORTHCOM**. When directed by the President, CDRUSNORTHCOM is responsible for conducting military operations within the USNORTHCOM AOR utilizing forces to deter, detect, or defeat an incursion into sovereign territory. CDRUSNORTHCOM has COCOM over Army, Air Force, and Marine Corps component headquarters. When forces are attached to the command for HD operations, the deployment order (DEPORD) will establish command relationships. CDRUSNORTHCOM determines the appropriate joint command and control (C2) structure to employ these forces. CDRUSNORTHCOM may retain direct C2 of forces as the joint force commander (JFC), designate an existing joint task force (JTF) commander, or establish a new subordinate JTF. CDRUSNORTHCOM and subordinate JTF commanders will normally organize forces around a joint construct with functional component commanders. However, CDRUSNORTHCOM may conduct HD operations using any combination of subordinate JFCs and functional component, Service component, single Service task force (normally assigned to the Service component), or specific operational forces necessary to accomplish the mission. Figure II-2 provides the USNORTHCOM C2 structure.

*For additional information on C2, see JP 1,* Doctrine for the Armed Forces of the United States.

(a) **C2 for HD Air Operations in the USNORTHCOM AOR**. C2 for HD air operations in the USNORTHCOM AOR is complex. When the NORAD OA and the USNORTHCOM AOR overlap, NORAD normally retains authority for the aerospace control and aerospace warning missions. For US-only air operations within CONUS Commander, Air Forces Northern (AFNORTH) may be designated the joint force air component commander (JFACC). Close coordination between the JFACC and NORAD is essential for synchronization of operations. For US-only air operations in Alaska, the Commander of the combined US-Canadian Alaskan NORAD Region (ANR) may be designated the JFACC.

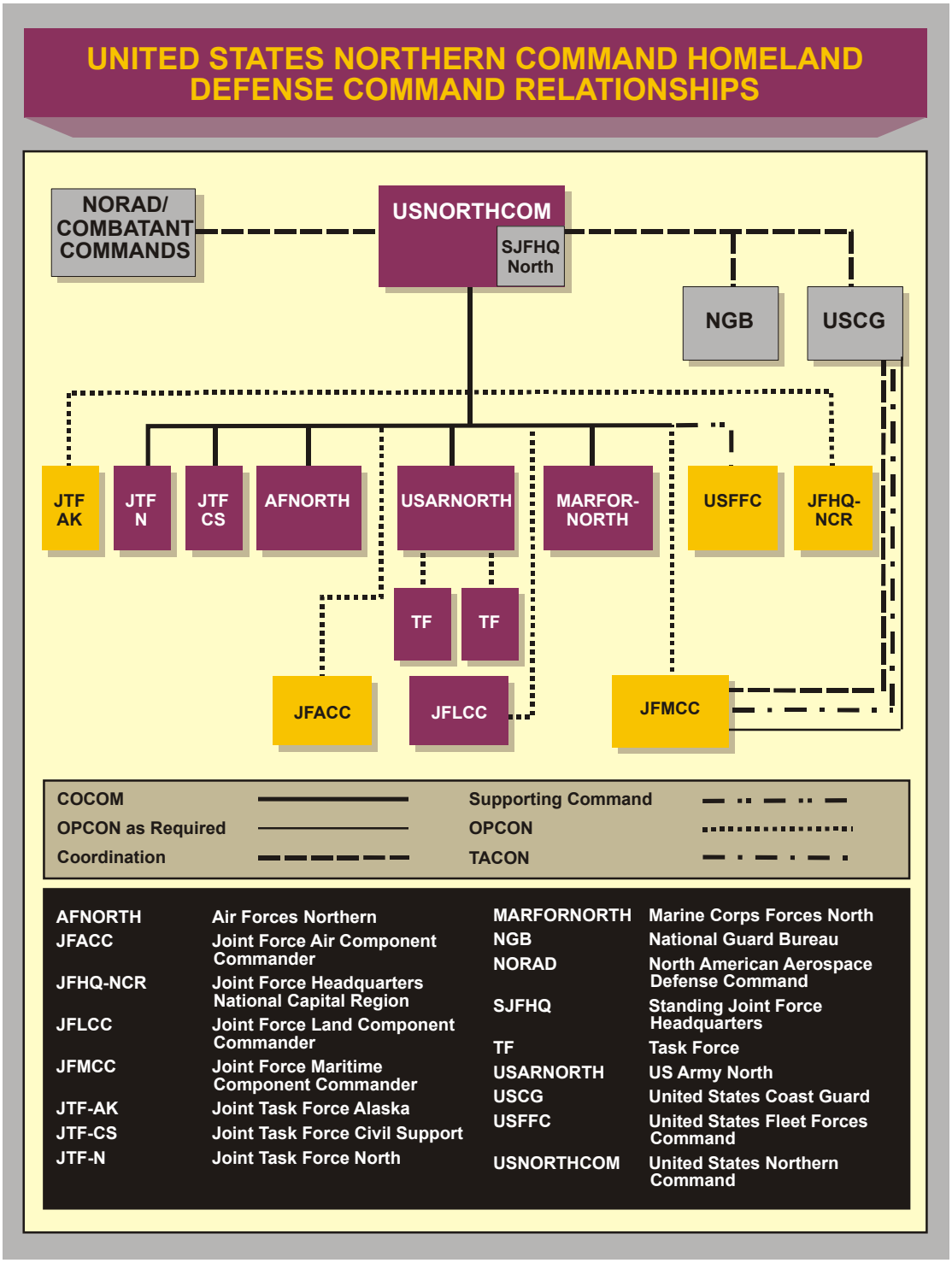



**Figure II-2. United States Northern Command Homeland Defense Command Relationships**

(b) **C2 for HD Land Operations in the USNORTHCOM AOR**. Land defense forces generally plan and execute HD land operations using a mix of Service assets, primarily those of the Army and Marine Corps. Operations can be conducted through Service task forces or joint forces. Force size, composition and C2 relationships depend

upon the situation and mission requirements. Commander, US Army North (USARNORTH) generally is responsible for conducting HD land operations and may also be designated the joint force land component commander (JFLCC). USARNORTH provides two deployable task forces that become JTFs when augmented. Marine Corps Forces North (MARFORNORTH) can provide a functional component headquarters, with augmentation. If the Marine Corps component commander is assigned functional component commander responsibilities, execution of HD missions will normally be accomplished by an assigned Marine air-ground task force.

(c) **C2 for HD Maritime Operations in the USNORTHCOM AOR**. Commander, US Fleet Forces Command (COMUSFLTFORCOM) is a supporting commander to CDRUSNORTHCOM and is designated as the joint force maritime component commander (JFMCC). The flag officer serving as Commander, Coast Guard Atlantic Area serves separately as Commander, Coast Guard Defense Force East (CGDEFOR EAST). Additionally, Commander, Coast Guard Pacific Area serves separately as Commander, Coast Guard Defense Force West (CGDEFOR WEST). US Coast Guard (USCG) forces under USCG Atlantic and Pacific area commanders may be designated operational control (OPCON) or TACON under the JFMCC, as required. The *Memorandum of Agreement Between the Department of Defense and the Department of Homeland Security for Inclusion of the US Coast Guard in Support of Maritime Homeland Defense* and its annexes contain the specific C2 structure and relationships that ensure USNORTHCOM, through the JFMCC, is able to effectively bring all available resources to bear in conducting maritime operations to deter, detect and defeat threats and aggression against the US, its territories, and interest within the USNORTHCOM AOR.

(d) **C2 for HD Special Operations in the USNORTHCOM AOR**. C2 relationships for SO are often complex. Commander, US Special Operations Command (CDRUSSOCOM) is assigned responsibility to lead, plan, synchronize, and as directed, execute global operations against terrorist networks. SOF in the US are normally under COCOM of CDRUSSOCOM. When directed, CDRUSSOCOM relinquishes OPCON/TACON of US based SOF and OPCON/TACON is assumed by CDRUSNORTHCOM for HD operations in the USNORTHCOM AOR. Under certain circumstances, regardless of AOR, CDRUSSOCOM will exercise OPCON of SOF conducting operations in support of the global war on terrorism. C2 arrangements for SOF should be carefully delineated in operation orders and execute orders (EXORDs).

(e) **Standing Joint Force Headquarters North (SJFHQ-North)**. SJFHQ-North is a standing joint C2 element within the USNORTHCOM staff. When USNORTHCOM is in routine, non-crisis operations, it functions as a combat operations staff organization that monitors and assesses activities that affect the AOR. When a crisis occurs, SJFHQ-North is prepared to immediately execute contingency operations by either standing up a JTF or augmenting the staff of a new or existing JTF or single-Service task force.

(f) **Joint Force Headquarters National Capital Region (JFHQ-NCR)**. JFHQ-NCR plans, coordinates, maintains situational awareness, and as directed, employs

forces for land and maritime HD in the National Capital Region (NCR) to safeguard the Nation's capital. NORAD provides air sovereignty protection to USNORTHCOM and JFHQ-NCR in the NCR through its aerospace and maritime warning and aerospace control missions and through the NCR integrated air defense system (NCR-IADS).

(g) **Joint Task Force Alaska (JTF-AK)**. JTF-AK is comprised of Alaskan Command (ALCOM) personnel, a subunified command of US Pacific Command (USPACOM). Placed under the OPCON of USNORTHCOM for HD (and CS) operations, JTF-AK is responsible for preventing, deterring, defending, and defeating national security threats within the Alaska joint operations area (JOA) as well as fulfilling FP requirements within the JOA.

(h) **Joint Task Force North (JTF-N)**. JTF-N supports federal LEAs in the interdiction of suspected transnational threats within and along the approaches to CONUS. During operations, active duty military forces are placed in support of a federal agency with lead responsibility. JTF-N contributes to HD by deterring, detecting, monitoring, and supporting the interdiction of suspected transnational threats. The organization also fuses and disseminates intelligence; contributes to the common operational picture; coordinates support to principal federal agencies; and supports security cooperation initiatives to secure the homeland and enhance regional security.

(i) **Joint Task Force Civil Support (JTF-CS)**. JTF-CS plans and integrates DOD support to the designated primary agency for CBRNE consequence management (CM). JTF-CS contributes to HD as the only dedicated military C2 organization focused on the CM core element of DOD's active, layered defense to reduce the effects of WMD attack or event and assists in the restoration of essential operations and services.

(j) **Ad hoc USNORTHCOM Joint Task Force.** When combat forces for a joint HD operation are attached to USNORTHCOM, CDRUSNORTHCOM may decide to employ these forces, based upon the scope and objectives of the operation to establish one or more new subordinate JTFs. JTF-AK and JFHQ-NCR (when designated a JTF) could have combat forces attached to conduct HD operations within their respective JOAs. However, while USNORTHCOM has standing JTFs, these commands have specific operational missions and may not have the personnel or expertise to manage a new HD operation. CDRUSNORTHCOM may task assign component command headquarters or supporting commanders to provide the core of a new JTF headquarters with augmentation from the other Services.

*For detailed information on consequence management see JP 3-28*, Civil Support *and JP 3-41*, Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives Consequence Management.

(3) **Commander, USPACOM (CDRUSPACOM)**. CDRUSPACOM integrates and synchronizes a broad range of military activities to defend the homeland against attacks and aggression. These activities include the protection of the domestic population and DCI of the United States and its territories. It also includes the domestic population and critical

infrastructure of the sovereign nations, commonly called freely associated states, under the Compact of Free Association located in the USPACOM AOR. These nations include the Federated States of Micronesia, the Republic of the Marshall Islands, and the Republic of Palau. Figure II-3 identifies the US territories located in the Pacific and the nations included in the Compact of Free Association. Additionally, in support of USNORTHCOM, military and intelligence operations contribute to the active, layered defense in-depth of the western approach to CONUS and Alaska.


**Figure II-3. US Territories, Possessions, and Freely Associated States Located in the US Pacific Command Area of Responsibility**

(a) When a HD event occurs in the Pacific AOR, USPACOM is the supported command. Support relationships are coordinated among CCDRs with geographic HD responsibilities for all HD events. CDRUSPACOM approaches HD through a functional construct as shown in Figure II-4. The Commanding General, US Army Pacific (CG USARPAC) assumes functional component commander responsibilities as the land component commander for the USPACOM portion of the US and its territories. Dual-hatted as the Commander JTF-Homeland Defense (CDR JTF-HD), CG USARPAC responsibilities include situational awareness of operations conducted against a direct threat

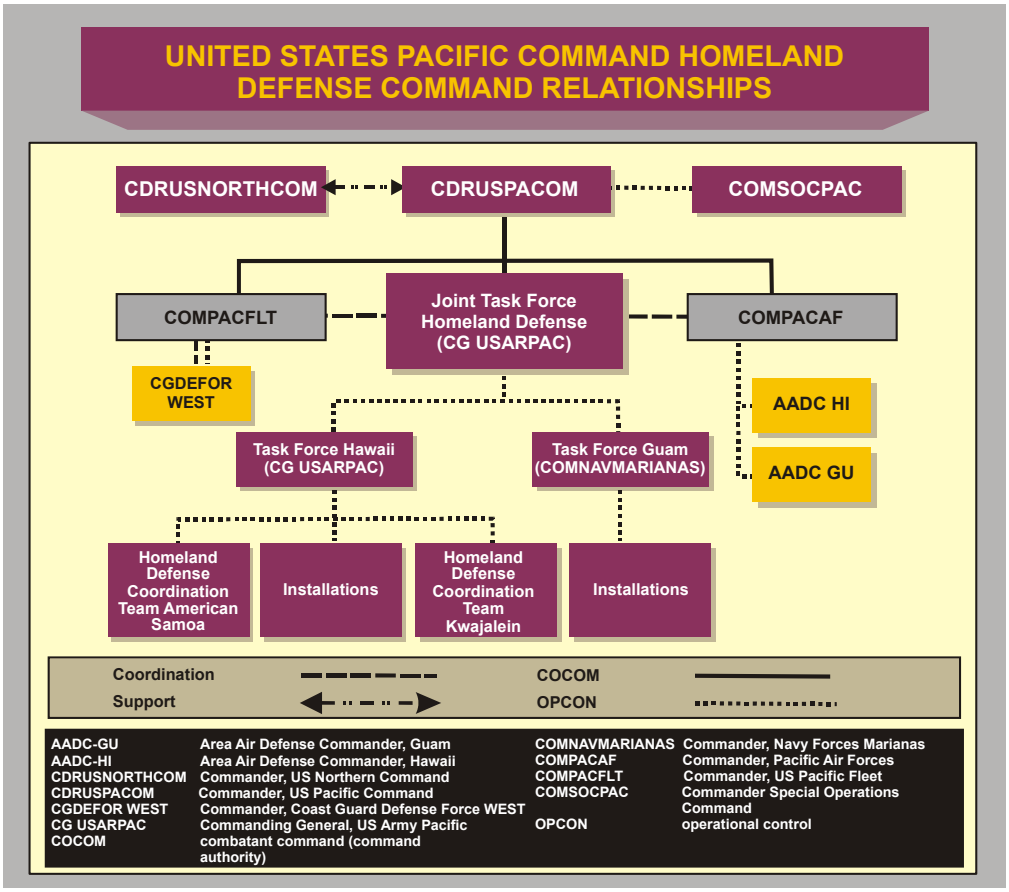



**Figure II-4. United States Pacific Command Homeland Defense Command Relationships**

to the JTF-HD JOA (this includes CBRNE CM and CS) and working closely with applicable federal, state, tribal, and local agencies when orchestrating DOD operations. All HD activities are coordinated with USNORTHCOM across AOR boundaries, including those concerning Hawaii and Alaska.

(b) The Commander, Pacific Air Forces (COMPACAF) assumes functional component commander responsibilities as the air component commander for the USPACOM portion of the US and its territories. In addition to the air responsibilities, COMPACAF assumes the responsibility for HD operations for space for the USPACOM portion of the US and its territories. Commander, Pacific Fleet (COMPACFLT), as the JFMCC, assumes functional component commander responsibilities as the maritime

component commander for the USPACOM portion of the US and its territories and coordinates maritime responsibilities with the Commander, Coast Guard Pacific Area, who serves separately as CGDEFOR WEST. This includes planning and execution of maritime operations and security cooperation. US Coast Guard (USCG) forces under USCG Pacific area commanders may be designated either OPCON or TACON to the JFMCC, as required. The *Memorandum of Agreement Between the Department of Defense and the Department of Homeland Security for Inclusion of the US Coast Guard in Support of Maritime Homeland Defense* and its annexes contain the specific C2 structure and relationships that ensure USPACOM, through the JFMCC, is able to effectively bring all available resources to bear in conducting maritime operations to deter, detect and defeat threats and aggression against the US, its territories, and interest within its AOR.

(c) To assist the CDR JTF-HD in accomplishing HD missions, organizations such as the USPACOM Joint Intelligence Operations Center, Joint Interagency Task Force West, Special Operations Command Pacific (SOCPAC), and USPACOM Service components provide intelligence, interagency coordination, and military forces.

(d) SO conducted in the USPACOM AOR are normally under the COCOM of CDRUSPACOM while OPCON is exercised through the theater SO component, SOCPAC. SOCPAC is tasked to conduct regional activities that may support future operations.

(e) As shown in Figure II-4, the CDR JTF-HD employs two task forces and subordinate coordination teams in two Pacific operational areas associated with Task Force Hawaii and Task Force Guam. These forces, along with local installations, conduct HD operations and respond to support requests by civil authorities.

(4) **Commander, USSOUTHCOM (CDRUSSOUTHCOM)** integrates and synchronizes military activities to defend the Commonwealth of Puerto Rico and the territory of the US Virgin Islands against attacks and aggression. CDRUSSOUTHCOM's military activities in South and Central America and the Caribbean basin also contribute to the active, layered defense in-depth of the southern approaches to CONUS.

(a) CDRUSSOUTHCOM approaches HD through a functional construct as shown in Figure II-5. The CCDRs with geographic HD responsibilities coordinate to provide mutual support for HD. Commander, US Army South (USARSO) assumes functional component commander responsibilities as the land component commander for the USSOUTHCOM portion of the US and its territories. Commander, US Air Forces South assumes responsibilities as the air component commander (to include space) for the USSOUTHCOM portion of the US and its territories and coordinates with NORAD for air defense of the US Virgin Islands and Puerto Rico. Commander, US Navy Forces Southern Command (USNAVSO) assumes responsibilities as the maritime component commander for the USSOUTHCOM portion of the US and its territories.

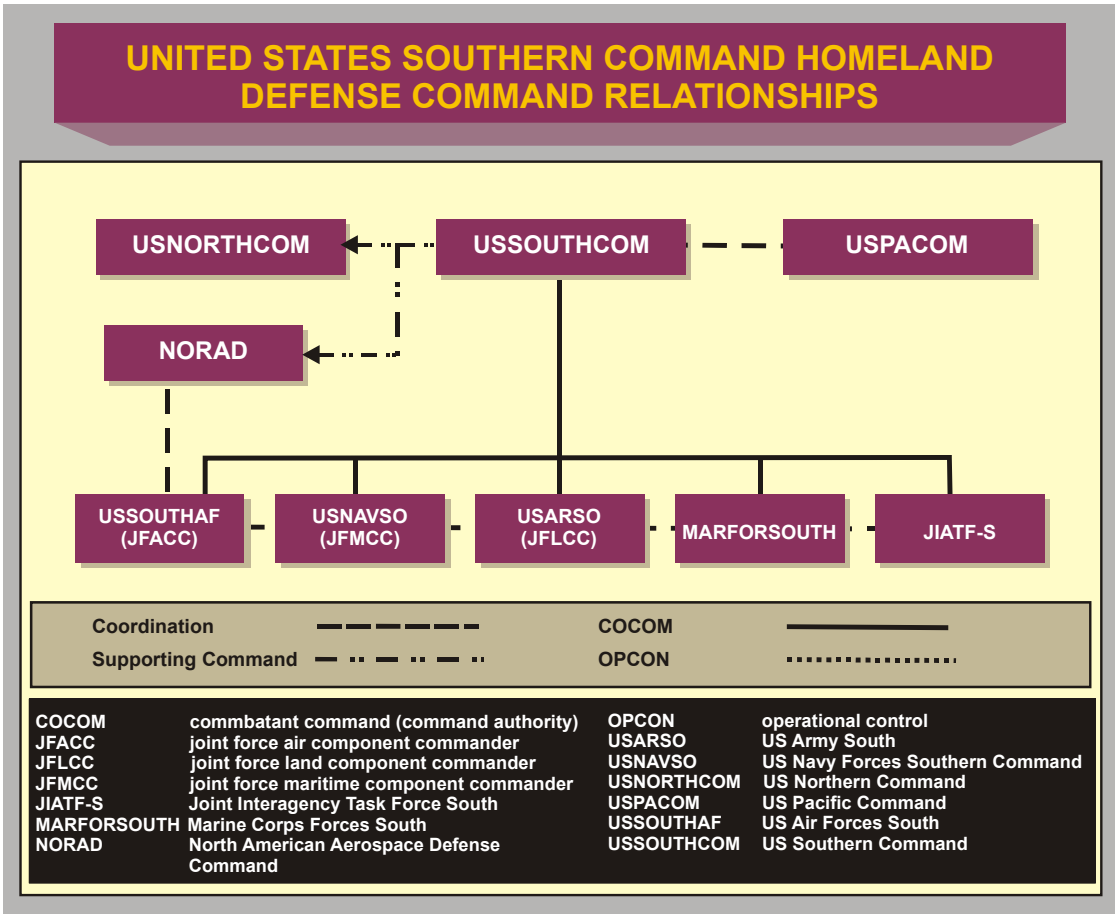



**Figure II-5. United States Southern Command Homeland Defense Command Relationships**

(b) The Joint Interagency Task Force South, Special Operations Command South, and US Marine Corps Forces South (MARFORSOUTH) provide support for HD missions in Puerto Rico and the US Virgin Islands.

(5) **Commander, US European Command (CDRUSEUCOM) and Commander, US Central Command (CDRUSCENTCOM)**. CDRUSEUCOM and CDRUSCENTCOM play a vital role in HD by supporting the CCDRs with geographic HD responsibilities. Specifically, they provide a forward presence to obtain information on potential adversaries that may be planning attacks on the homeland and they deny adversaries air, land, and maritime approaches to the homeland. They also conduct operations within their AORs in support of HD.

c. **Functional Combatant Commander Responsibilities**

(1) **Commander, US Strategic Command (CDRUSSTRATCOM).** CDRUSSTRATCOM is responsible for providing the nation with global deterrence capabilities and synchronizing DOD efforts to combat adversary weapons of mass destruction worldwide. Specifically, CDRUSSTRATCOM is responsible for the following activities associated with HD:

(a) Planning, integrating and coordinating global missile defense operations and support.

(b) Integration of global strike planning and C2 in support of theater and national objectives. US Strategic Command (USSTRATCOM) normally supports the GCCs in the conduct of global strike missions, unless otherwise directed by the President.

(c) Planning, integrating, and coordinating global DOD IO activities that directly support national objectives to include computer network operations, as well as defense of DOD computers and computer networks of the Global Information Grid (GIG).

(d) Planning, integrating, and coordinating ISR in support of strategic and global operations.

(e) Planning and implementing security assistance relating to military space operations, and providing assessments.

(f) Planning, integrating, and synchronizing DOD combating WMD efforts in support of national security objectives.

(2) **Commander, US Special Operations Command**. CDRUSSOCOM leads, plans, synchronizes, and as directed, executes global operations against terrorist networks. US Special Operations Command (USSOCOM) also trains, organizes, equips and deploys combat ready SOF in support of other combatant commands. For HD, CDRUSSOCOM serves as a supported or supporting commander for selected CT activities and serves as a supporting commander the CCDRs with geographic HD responsibilities within their respective AORs.

(3) **Commander, US Transportation Command (CDRUSTRANSCOM)**. CDRUSTRANSCOM provides airlift and tanker forces, as well as base opening and C2 capabilities to supported commanders. For HD operations, CDRUSTRANSCOM provides, upon request, a director of mobility forces to advise on air mobility operations. CDRUSTRANSCOM serves as the supporting commander to CDRUSSTRATCOM for designated global strike and selected CT activities for HD.

(4) **Commander, US Joint Forces Command (CDRUSJFCOM).** CDRUSJFCOM's role in HD is to provide support as joint force provider, integrator, and trainer. Through joint concept development and experimentation the command also provides concept validation for the combatant commands.

d. **Reserve Component Responsibilities**. NG (in a Title 10 USC status) and reserve forces are collectively referred to as RC and are integral to the accomplishment of peacetime missions and conflict prevention. They consist of the Army National Guard of the United States (ARNGUS), the US Army Reserve (USAR), the US Navy Reserve (USNR), the US Marine Corps Reserve (USMCR), the Air National Guard of the United

States (ANGUS), the US Air Force Reserve (USAFR), and the USCG Reserve (USCGR). **Guidelines for the utilization of RC forces are found in Title 10 USC. Title 32 USC contains guidelines for the training of the Army National Guard (ARNG) and the Air National Guard (ANG), as well as their domestic use for homeland defense activities.**

(1) **National Guard Bureau (NGB)**. NGB is a , joint bureau of the Department of the Army and Department of the Air Force, that serves as the NG channel of communications for all matters pertaining to the NG between the Army and Air Force, the 50 states, District of Columbia, Commonwealth of Puerto Rico, Guam, and the US Virgin Islands. While the NGB does not exercise operational authority, it provides coordination and communication between the states, DOD, and other federal agencies. This role is crucial when the states conduct domestic operations in a Title 32 USC status. The NGB, under provisions of Title 10 USC, Section 10503 is responsible for the following matters:

(a) Allocating unit structure, strength authorizations, and other resources to the ARNGUS and the ANGUS.

(b) Prescribing the training discipline and training requirements for the ARNG and the ANG and the allocation of federal funds for the training of the ARNG and the ANG

(c) Ensuring that units and members of the ARNG and the ANG are trained by the states in accordance with approved programs and policies of, and guidance from, the Chief, National Guard Bureau (CNGB), the Secretary of the Army, and the Secretary of the Air Force.

(d) Monitoring and assisting the states in the organization, maintenance, and operation of NG units so as to provide well-trained and well-equipped units capable of augmenting the active forces in time of war or national emergency.

(e) Planning and administering the budget for the ARNGUS and the ANGUS.

(f) Supervising the acquisition and supply of, and accountability of the states for, federal property issued to the NG through the property and fiscal officers designated, detailed, or appointed under Title 32 USC, Section 708.

(g) Granting and withdrawing, in accordance with applicable laws and regulations, federal recognition of (1) NG units, and (2) officers of the NG.

(h) Establishing policies and programs for the employment and use of NG technicians under Title 32 USC, Section 709.

(i) Supervising and administering the Active Guard and Reserve program as it pertains to the NG.

(j) Issuing directives, regulations, and publications consistent with approved policies of the Army and Air Force, as appropriate.

(k) Facilitating and supporting the training of members and units of the NG to meet state requirements.

(l) Such other functions as the Secretaries may prescribe.

(2) **Chief, National Guard Bureau.** The CNGB, is the principal advisor on NG matters to the Secretaries of the Army and Air Force and to the Chiefs of Staff of the Army and Air Force. This role does not include combatant command (warfighting) authority, nor does it include the requirement to organize, conduct training, and equip.

(3) **National Guard.** The NG has both state and federal missions and is at different times under the C2 of the governors or the President. Every NG member takes an oath to uphold the US Constitution and the constitution of his or her respective state. The NG trains under the control of the states according to the rules and regulations prescribed by the USG.

(a) The ARNG and ANG are established in 54 states and territories, including the Commonwealth of Puerto Rico, the Territory of the US Virgin Islands, the Territory of Guam, and the District of Columbia. The head of the NG in each state is the adjutant general, who reports to the governor. However, in the District of Columbia, the head of the NG is called the commanding general, and he or she reports through channels ultimately to the President of the United States. The adjutant general usually heads either a state department of military affairs or a combined state department of military affairs and emergency management. The adjutant general may have other duties under state law such as state director of homeland security.

(b) The NG is both part of the organized militia and the RC (when in Title 10 USC status). The ARNGUS and the ANGUS are the respective Service part of the RC. Every member belongs to either the ARNG or ANG of his or her state, and also to either the ARNGUS or the ANGUS. It is important to distinguish between NG forces acting under state authority and NG forces when called into federal service. The ARNGUS and ANGUS are RC organizations under the C2 of the President. The ARNG and ANG train for their federal military mission according to Title 32 USC, under state control as members of their respective state militias.

(c) A member of the National Guard can serve in three different statuses:

1. Title 10 USC Status – Federal Active Duty. The member is ordered to active duty under various sections of Title 10 USC. This status is almost always based on membership in the ARNGUS or ANGUS. The member's pay and allowances are federally funded, and the member is under federal C2. This is the status members always serve in outside the United States, whether for training or operational missions. When NG personnel or units are activated by order of the President under

Title 10 USC for HD missions, they respond under the same legal restrictions and C2 structures as active component (AC) forces to include the provisions of the Uniform Code of Military Justice (see Appendix A, "Transitioning Between Homeland Defense and Civil Support").

2. Title 32 USC Status – National Guard Duty. The member is ordered to duty under various sections of Title 32 USC. This status is used for both training and certain operational missions. The member's pay and allowances are federally funded, but the member is under state C2. For training, this status includes weekend drills, annual training, and certain other types of training paid out of reserve force appropriations. Under the authority of special statutes, this status is also used for certain operational missions, including CD missions, HD activities, and the WMD civil support teams.

3. State Active Duty Status. The member is ordered to state active duty under provisions of state law in the state where he or she is a member of the state NG. This status is used for state responses to natural and man-made disasters and civil disturbances. The member's pay and allowances are state funded, and the member is under state C2. The member's pay and allowances in some states may not be the same under state law as they are under federal law.

*For additional information on state active duty status in relation to CS, see JP 3-28*, Civil Support.

(d) Each state has a joint force headquarters (JFHQ), which integrates the ARNG and ANG resources. The JFHQs provide a focal point to interoperate jointly with combatant commands and any federal joint task forces that may perform HD (or CS) within a state's boundaries.

(e) JTFs in each state facilitate the joint employment of state NG resources under the JFHQ-state for operational missions in either Title 32 USC status or state active duty.

(4) **Reserve Forces.** Each of the seven parts of the RC is structured and operated in a manner similar to its respective AC counterpart. Unlike the ARNGUS and ANGUS, the remaining five RC organizations (USAR, USNR, USAFR, USMCR, USCGR) operate under the same C2 relationships in both peacetime and wartime and do not have State-specific relationships. When called to active duty, RC forces conduct HD operations under Title 10 USC guidelines exactly as AC forces. While on active duty, members of the USAR, USNR, USAFR, USMCR and the USCGR are subject to the provisions of the Uniform Code of Military Justice. Reserve forces are called to active duty through the mobilization process.

*For additional information on the RC mobilization/demobilization process, see JP 4-05.1*, Manpower Mobilization and Demobilization Operations: Reserve Component (RC) Call-up.

## 3. Interagency Responsibilities and Considerations

a. **Interagency Coordination and Interoperability.** HD operations are conducted in a complex environment that is characterized by an operational environment with thousands of different jurisdictions (federal, state, tribal, and local), many agencies and organizations, and several allies and coalition partners. This necessitates coordinated and integrated operations with our HD partners to ensure the mutual security of our nations, safety of our populations, and viability of our critical infrastructure.

(1) The interrelationship between HS, HD and CS operations, and the potential for transition between the missions, creates a dynamic and fluid environment where interagency coordination and interoperability become a focal point. Giving the initiative to an adversary, because seamless operations with interagency partners could not be coordinated due to an inability to cooperate or be interoperable, is unacceptable.

(2) Although interagency coordination and interoperability can at times be a significant challenge and take considerable effort, it also provides numerous benefits and "force multipliers" for DOD, CCDRs, and HD partners. For example, NORAD, DOD, the Department of Transportation's (DOT's) Federal Aviation Administration (FAA), and DHS (USCG, Transportation Security Administration (TSA), and Customs and Border Protection – Office of Air and Maritime Operations) have enhanced the integration and interoperability of systems and sensors; expanded information sharing and the number of liaison personnel in key operations centers; implemented interagency air defense related exercises; and, enhanced real-time warning conferences, all of which have improved HD (and CS) capabilities.

b. **The Interagency Process and Coordinating Organizations**

(1) Interagency coordination is conducted at the strategic, operational, and tactical levels. At the strategic level**,** DOD interaction and participation is largely performed by senior DOD and military leaders and their support staff, to include SecDef, Deputy Secretary of Defense, CJCS, and Vice-CJCS in such key committees as the National Security Council (NSC), the Homeland Security Council (HSC), including their respective Principals Committee and Deputies Committee, and the various policy coordination committees. CCDRs with appropriate SecDef and CJCS direction, approval, and coordination, may interact with and provide input to select policy coordination committees on significant national and/or theater level issues on which the commander can add unique insight and value added recommendations.

(2) Homeland Security Council. The HSC is a national-level multiagency coordination entity to advise and assist the President on HS and other policy issues. Organized similar to the NSC, the HSC consists of the HSC Principals Committee, the HSC Deputies Committee and various policy coordination committees.

(3) NSC/HSC Policy Coordinating Committees (PCCs). The PCCs are the primary forums used across the interagency for coordination of policy, including that associated with maritime security, aviation security, and border and transportation security. Additionally, the

Counterterrorism Security Group, attended by the Joint Staff and appropriate Office of the Secretary of Defense (OSD) representatives, provides an operationally focused forum to coordinate USG activities associated with terrorist threats globally.

(4) National Operations Center. The National Operations Center (NOC) was established in May 2006 with the approval of an NRP change that linked together and integrated the functions of the former Homeland Security Operations Center, the Office of Intelligence and Analysis (OI&A), the National Response Coordination Center, the National Infrastructure Coordination Center, and the Planning Element from the Incident Management Planning Team (IMPT). The NOC provides critical functions and capabilities that are central for the DHS to lead the unified national effort to secure America and implement domestic incident management authorities, roles and responsibilities mandated by Homeland Security Presidential Directive (HSPD)-5, *Management of Domestic Incidents* and the Homeland Security Act. The NOC's mission is to serve as the primary national level hub for domestic situational awareness, common operating picture, informational fusion, information sharing, communications, and operations coordination pertaining to the prevention of terrorist attacks and domestic incident management.

(a) The NOC is a 24x7, multiagency operations center that collects all threat and all hazards information from federal, state, tribal, local, private-sector, and open sources from across the US and abroad.

(b) The NOC serves as the National Fusion Center collecting and immediately fusing all-source information to quickly determine if there is a terrorism nexus and supports OI&A in deliberate fusion.

(c) The NOC fuses state fusion center, law enforcement, national intelligence, emergency response, and private sector reporting and disseminates homeland security information to appropriate intelligence and law enforcement agencies, other security partners, and the DHS and White House/HSC leadership.

(d) The NOC is the primary conduit to the White House and the Secretary of Homeland Security for domestic situational awareness for the prevention of terrorist attacks and domestic incident management within the US.

(e) The NOC maintains domestic situational awareness through a common operating picture.

(f) The NOC is comprised of five elements and operates as a matrix organization:

1. NOC-Watch (Multiagency)

2. NOC-IA (Intelligence)

3. NOC-PE (Planning Element/IMPT)

4. NOC-NRCC (Federal Emergency Management Agency [FEMA]: National Response Coordination Center)

5. NOC-NICC (National Infrastructure Coordinating Center)

(5) The combatant command interagency process complements and supports the higher level or strategic interagency process, and may involve such key elements as joint interagency coordination groups (JIACGs); security cooperation programs, plans and initiatives; country team interaction and coordination; and annex V (Interagency Coordination) to formal OPLANs and CONPLANs; all designed to enhance information sharing, effective joint and interagency planning, and maximize coordinated operations. The interagency coordination process is essential when HD operations are conducted in proximity to our domestic population and critical infrastructure.

(6) Operational coordination is conducted within appropriate joint force command centers and their corresponding federal, state, tribal, or local interagency facilities and IGOs, NGOs, and/or the private sector. Expedited procedures and protocols for coordination of USG defense and security activities are vital to protection of the homeland.

c. **Importance of Interagency Communications, Coordination, Collaboration, and Cooperation in Homeland Defense Operations.**

(1) Within the US homeland, DOD and US military forces must effectively deal with time compression of actions, potential impact on US domestic population and DCI, and unique legal and policy guidelines. These forces face continuous media scrutiny, must be sensitive to sovereignty and jurisdictional considerations, and mindful of political dimensions of a domestic response, yet responsive enough to deal with the varied threats to the homeland. This environment necessitates an effective interagency process and program.

(2) Partner agencies and organizations of the USG in the homeland and overseas support and assist DOD in the conduct of HD operations. For example, the intelligence community (IC) and associated agencies (e.g., Central Intelligence Agency [CIA], Defense Intelligence Agency [DIA], National Security Agency [NSA], National Geospatial-Intelligence Agency [NGA]) identify, describe, and quantify external threats; DOJ/Federal Bureau of Investigation (FBI) and partner law enforcement, counterintelligence, and security/FP agencies identify internal threats and conduct CT, security/FP, and counterespionage activities; DOT/FAA radars locate and identify aircraft; and DHS conducts operations in the maritime, border, and air security areas. These agencies perform functions supportive of DOD's HD mission and are essential to the overall HD effort. However, to achieve unified action for HD, it is imperative that joint and interagency, communication, coordination, collaboration, and cooperation be optimized through the planning, training, and execution of any HD effort.

(3) Although the leads for HD (DOD) and CS (e.g., DHS and DOJ) are different, the distinction between the two operational activities may not easily be defined or discerned. There may be cases where HD and CS events take place concurrently, or the main threat and therefore the agency lead, transitions from one agency to the other. Therefore, the need to

establish workable and effective interagency relationships and partnerships, in advance of a crisis or contingency, is critical. For example, DOD may support DHS activities in the US portion of the maritime domain, requiring continuous coordination between department-level, operational, and tactical organizations conducting operations. The MOTR Plan acts to mitigate overlap issues between HD and HS activities by providing a method for interagency integration (see Chapter V, "Maritime Operations" and Appendix A, "Transitioning Between Homeland Defense and Civil Support" for more information on the MOTR Plan and the relationship between HD and HS). To fully develop and verify such relationships and partnerships, an active interagency coordination program, backed-up by annual joint and interagency exercises or operations, is required.

d. **Combatant Command Tools and Methods for Interagency Communications, Coordination, Collaboration, and Cooperation.** Combatant commands that operate in the homeland and perform HD missions (or CS missions) need to take full advantage of the complete set of interagency and DOD "tools and methods" to maximize mission success; enhance coordinated and seamless operations with our HD mission partners; and, eliminate/minimize any adverse impact on the US population and critical infrastructure. Some specific tools and methods which combatant commands can use include the following:

(1) **Interagency Coordination Offices.** An interagency coordination office may be established as a staff element within a combatant command headquarters with the mission of facilitating coordination of interagency activities to promote mutual understanding and unity of effort. **Each CCDR organizes or tailors the interagency coordination office and/or function differently based on the particular mission(s), AOR, and requirements.** During an exercise or incident, this staff element expands to use the full capabilities of assigned or attached agency representatives and command liaison officers (LNOs) to reach-back and provide situational awareness to the CCDR and staff. A notional example of how an interagency coordination office conducts business is illustrated in Figure II-6.

(2) One construct for interagency coordination operations is of three areas of influence, all nested together. The inner area represents day-to-day activities of permanent party members on the interagency coordination staff. Day-to-day, these staff members provide situational awareness and advice to the commander and staff pertaining to interagency issues and implications. They attend command and interagency meetings, conferences, and exercises to build relationships with other agencies and commands. They also write the interagency portion of military plans and review DOD and interagency documents to ensure that interagency and DOD equities are considered from their combatant command perspective.

(3) **Interagency Coordination Group (IACG)/Interagency Planning Cell (IPC).** The IACG is the interagency incident management group for the JIACG during contingencies or exercises, and provides an interagency facilitation and planning capability on a 24-hour, 7-day per week basis, if required. The IACG is formed by members from the interagency coordination office (which provides people, resources, and reach-back

capability for additional subject matter expertise) and is augmented by available and required agency representatives and command LNOs. These personnel collaborate to provide the CCDR and staff a clear picture of interagency activities and their implications. The IACG mission is to integrate and synchronize interagency activities to ensure mutual understanding, unity of effort, and full spectrum support. A group similar to the IACG is the IPC, which is activated upon receipt of CJCS's warning or alert order or at the direction of the CCDR. The IPC is established to provide timely advice to the supported CCDR about the capabilities/resources of other agencies in the HD effort and/or associated CS requirements resulting from an attack on the homeland. An IPC will enable a coherent and efficient planning and coordination effort through the participation of interagency subject

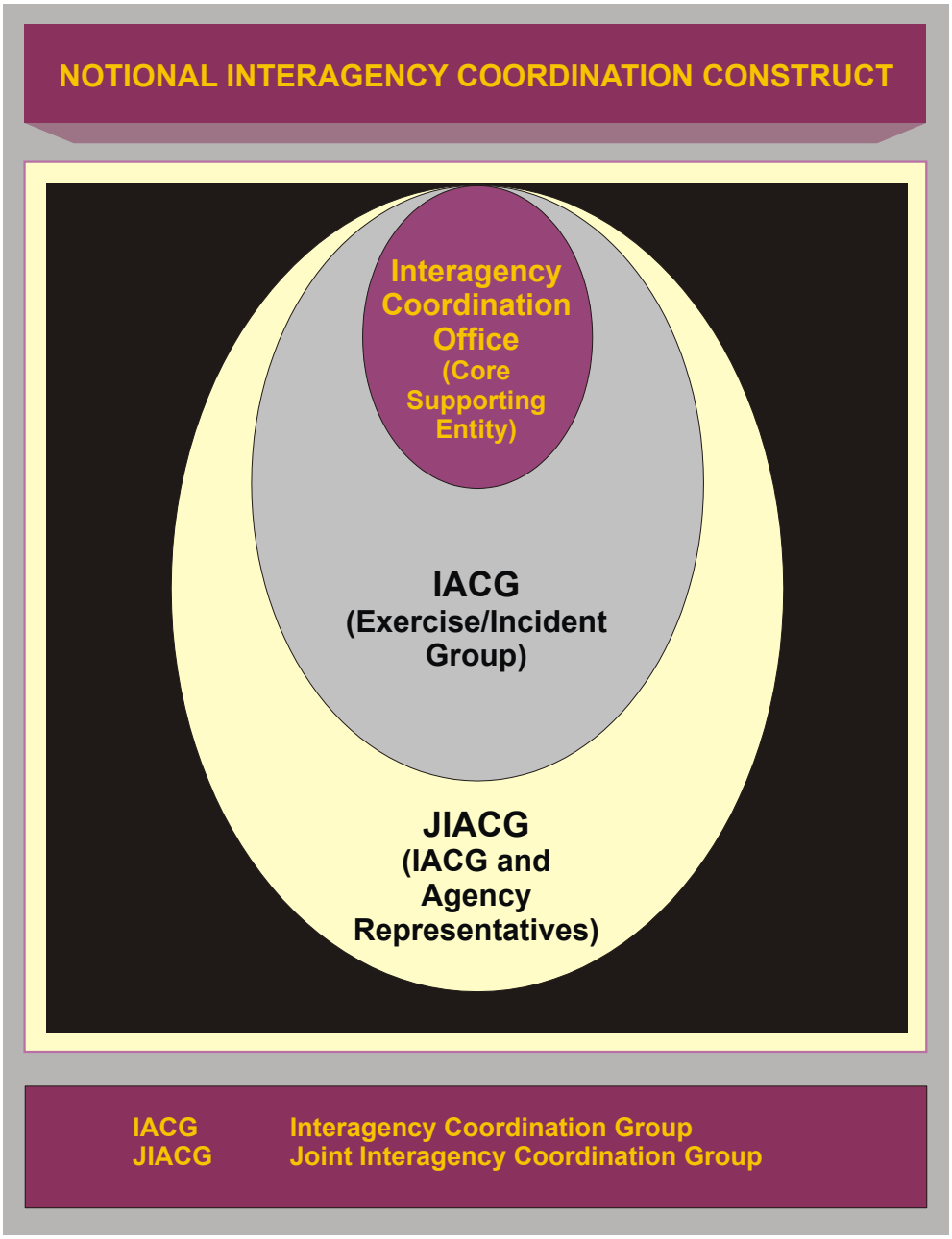



**Figure II-6. Notional Interagency Coordination Construct**

matter experts. Whether an IACG or an IPC, the element provides the CCDR an interagency action group focused on contingencies that can assist and enhance the command's planning and execution efforts.

(4) **Joint Interagency Coordination Group.** The mission of the JIACG is to set the conditions for operational success by synchronizing and at times integrating activities with the state and local governments, multiple national and intergovernmental agencies, and partner commands to ensure mutual understanding and unity of effort across the full range of military operations. It is the CCDR's primary interagency forum consisting of agency representatives, command LNOs, and staff representatives collaborating to share information, analyze ongoing activities, and anticipate future interagency actions, implications, and/or consequences. It's important to note that the JIACG does not replace or supplant the normal combatant command operations and/or staffing process, but is a force multiplier to those processes. During a crisis or contingency, the operational arm of the JIACG is the IACG/IPC, which can be set up to operate 24-hours, 7-days per week, and is sourced by interagency qualified personnel from the interagency coordination office and JIACG membership, and is tailored to meet interagency operational and/or planning requirements for the commander and staff.

(5) **Agency Representatives and Command Representatives.** Subject matter experts from key partner agencies and commands facilitate effective two-way communication, coordination, and cooperation. A formally established liaison and representative link between the combatant command and the partner agency is mutually beneficial. Specific focus should be on agency or command LNOs whose organizations play a key part in successful and seamless execution of HD operations. Additionally, in an HD event or operation, CM response actions may be required due to significant resulting damage. Regardless of mission, having key partner agency and command representatives will be essential for the CCDR conducting operations on US territory. Representatives from organizations such as DHS, DOJ, DOT, Department of Energy (DOE), Department of Health and Human Services (DHHS), CIA, and from DOD agencies should be considered as a starting point. Equally important, combatant commands may locate a command representative or LNO at key partner agencies commensurate with their operational requirements. Agency representatives or command LNOs are more effective when they have access to command leadership, key staff, and key working groups. "On-the-ground" agency representatives and command LNOs located at a combatant command should typically be located where they will be most usefully engaged, supportive of command activities, and beneficial to their parent agency or command. However, they also need to have an ongoing interface with the interagency coordination office and functions and actively participate in and support the JIACG and the IACG/IPC groups. This maximizes their participation in and support of the interagency process and benefit to their particular agency or combatant command. Information on other government agencies is provided in Appendix B, "Key Interagency Organizations."

e. **Interoperability – Importance of Effective Interagency Communications, Coordination, Collaboration, and Cooperation.** One of the most important facilitators of successful joint, and multinational operations or interagency coordination is the ability

to be interoperable and easily share pertinent information to effectively coordinate action. This is especially critical in HD operations where military operations may be conducted in close proximity to our domestic population and our critical infrastructure. Two elements are required for true interoperability: first is the intent and commitment to share information among HD partners; and second, that systems interface or work together to facilitate effective communications, information sharing, and coordination. It is vital for DOD, to be more than "administratively connected" to HD partner agencies. It is also essential to be operationally connected and interoperable to facilitate rapid and effective exchange of critical information and provide a dynamic environment for coordinating joint and interagency HD activities. Timely and accurate situation assessments and responses are important factors in saving lives and protecting infrastructure and property. The interagency partnership requires a common operational picture (COP) and interoperable systems. This is essential to ensure we can effectively conduct HD operations, while eliminating or minimizing injury to our domestic population and damage to our critical infrastructure. Chapter VII, "Other Supporting Operations and Enabling Activities" provides further discussion and guidance on improved information sharing.

*For further reference, see JP 3-08*, Interagency, Intergovernmental Organizations, and Nongovernmental Organization Coordination During Joint Operations (Vol 1 & 2).

### 4. Command and Control Considerations for Multinational Operations

Multinational operations include alliances or coalitions between two or more nations to better achieve common interests. To conduct the full range of HD operations, the CCDRs with geographic HD responsibilities are required to coordinate actions with all instruments of national power, as well as multinational and nonmilitary organizations. When a response force is resident within an alliance, the procedures and structure of the alliance will normally determine the strategic and operational level leadership. When a response force is based in a coalition (or a lead nation structure in an alliance), the designated lead nation will normally select both the strategic and operational level leadership. While the President and SecDef retain command authority over US forces it is sometimes prudent or advantageous (for reasons such as maximizing military effectiveness and ensuring unity of effort) to place appropriate US forces under the OPCON of a foreign commander to achieve specified military objectives.

*For further details (including restrictions) and additional information see, JP 1,* Doctrine for the Armed Forces of the United States *and JP 3-16*, Multinational Operations.

### 5. Synchronization and Integration of Homeland Defense Operations

a. Synchronization is the arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time. Integration should include military and civilian organizations as appropriate. The JFC must be fully cognizant of the strategic direction in order to establish the priorities, timelines, goals and objectives for HD missions that allow synchronization and

integration of air, land, maritime, space and supporting operations for unified action. DOD policies, international and command agreements, federal constitutional and statutory law, security cooperation plans (SCPs), and selected OPLANS provide guidance, which must be integrated by the CCDR to achieve synchronization.

(1) Command arrangement agreements (CAAs) establish procedures and delineate responsibilities between two or more CCDRs concerning mutual support, interface, and cooperation. They prescribe the arrangement necessary to support the employment of forces from one CCDR to another and the control of these forces operating within a specific AOR or JOA. CAAs may also delineate information and intelligence dissemination requirements to enhance coordination for planning and execution of cross-AOR operations. CAAs must remain consistent with DOD guidance as promulgated from SecDef and CJCS.

(a) The CAA between CDRUSNORTHCOM and CDRUSPACOM establishes the methodology under which transfer of forces between the two combatant commands is executed in support of HD (and CS) missions. Processes, C2 arrangements, and communication requirements are representative items addressed in the document (note that the transfer of maritime HD forces is also addressed in current EXORDs).

(b) The CAA between CDRUSNORTHCOM and CDRUSSOUTHCOM provides guidance for the planning and execution of operations conducted by both commands within the USNORTHCOM AOR. It prescribes the arrangements necessary for the control, support, and protection of forces operating, therein.

(2) Security cooperation is an enabler for HD. The United States seeks the cooperation of allies, coalition partners, and friends around the world to achieve its national security goals, and this cooperation is crucial to the defense of the homeland. CCDRs plan and conduct security cooperation activities to encourage and enable countries to work with the United States to achieve strategic objectives. Strengthening security relations with multinational partners increases their capabilities to contend with common challenges. Prevention and deterrence are crucial components of such a defense, but our friends and allies also require the capacity to defeat threats should they emerge.

(a) In the forward regions of the world, CCDRs and their components perform vital security cooperation activities with their partner countries that help provide the outer layer of HD.

(b) The CCDRs with geographic HD responsibilities have AORs with very different characteristics. In addition to its vast airspace, the USPACOM AOR is predominantly maritime and comprises considerable political, religious, cultural, social and economic diversity. It encompasses the Asia-Pacific region, comprising numerous sovereign nations and one-half of the earth's surface. The area includes five of the seven US security treaty allies, extensive international waters covered by international law, as well as US possessions and territories under US law, treaties or compacts. The US Southern Command (USSOUTHCOM) AOR consists of Latin American and Caribbean nations.

These nations are strategically important to our national security and economic future. The US is linked with these nations by geography, history, demography, economics and a shared security environment. Security within this region is being undermined by a growing number of threats, not the least of which is international illicit trafficking. The same routes that allow the flow of drugs also permit the movement of illegal aliens, weapons, and potentially terrorists. The USNORTHCOM AOR is primarily continental, with extensive land borders and coastal regions, including Canada, Mexico, and 49 US states (including Alaska) with differing legal and policy concerns as well as varying state-to-state mutual support agreements. Additionally, as the Alaska region is within the overlapping AORs of USPACOM and USNORTHCOM and the USSOUTHCOM AOR contains portions of the homeland in the Caribbean, it is essential for these GCCs to coordinate issues relating to HD. While the geographic, political, and diplomatic environments may be different, each CCDR employs a SCP to promote the assurance of allies and friends, the dissuasion of adversaries, and the deterrence of aggression.

1. **Engaging and Shaping**. Security cooperation enhances access, readiness, and training to build competent regional partners by improving their low to high-end capabilities. Through their SCPs, the CCDRs with geographic HD responsibilities seek to diminish the conditions that terrorists exploit and support activities to deny sanctuary to terrorists. The plans also strengthen and improve collaboration between joint commands, agencies at all levels of government, and regional partners. CCDRs with geographic HD responsibilities should address strategic communication in their security cooperation planning efforts.

2. **Enabling Continental Defense**. Effective security cooperation with North American partners (e.g., Canada, Mexico) is a vital aspect of HD. Achieving military and interagency interoperability and cooperation is key in enabling an effective defense of the continent. This capability begins by establishing and maintaining military relations, builds to combined education, training, and exercises, intelligence and information sharing, exchange of LNOs, and many other activities that enable multilateral operations to defend mutual homelands. CDRUSNORTHCOM's goal is to strengthen HD through a mutually beneficial North American defense partnership to counter terrorism and WMD and their consequences, while contributing to global US security objectives. Additionally, it is important to foster appropriate interagency relationships in order to leverage complementary capabilities and capitalize on limited resources.

(3) A number of initiatives and agreements exist that forge relationships and provide for multinational coordination in the defense of the homeland. A representative sample of these initiatives and agreements is provided below:

(a) Regional Maritime Security is a partnership of willing nations enhancing capabilities and leveraging capacities through unity of effort to identify, monitor and intercept transnational maritime threats consistent with existing international and domestic laws.

(b) Proliferation Security Initiative (PSI) is a Department of State led program that focuses on reducing WMD proliferation by deterring suppliers and customers, and making proliferation more costly and difficult.

(c) The Security and Prosperity Partnership of North America is an agreement between the United States, Canada, and Mexico, established to identify new avenues of cooperation to make the continent safer and more secure, businesses more competitive, and economies more resilient.

b. **Enhancing Multinational Coordination**. There are many activities that can increase our partners' capabilities to operate with us and create the conditions for establishing new multinational partnerships to contend with mutual challenges. SecDef's *Security Cooperation Guidance (SCG)* outlines a series of security activities that a CCDR can use to advance long-term security cooperation goals and objectives with multinational partners wherever feasible and mutually supportive. Some of these activities are presented below:

(1) Multinational exercises, training, education, and experimentation.

(2) Counternarcotics assistance.

(3) Counterproliferation and/or nonproliferation (includes Cooperative Threat Reduction, and International Counterproliferation Program).

(4) Defense and military contacts.

(5) Defense support to public diplomacy (for example, developing information programs in regional languages that complement other security cooperation activities).

(6) Security assistance.

(7) Other Programs and Activities – Regional Defense Counterterrorism Fellowship Program, Defense Environmental International Cooperation, etc.

*See the Secretary of Defense Security Cooperation Guidance for more information on security cooperation.*

c. In today's joint, multinational and interagency operating environment it is impossible to accurately view the contribution of any individual organization or capability in isolation from all others. This is particularly true when contemplating the complex environment within the homeland. Each may be critical to the success of the joint force, just as the joint force may be critical to interagency success. Each has unique capabilities that cannot be duplicated by other agencies. The challenge for the supported JFC is to integrate and synchronize the wide range of capabilities at his disposal into joint operations against the adversary.

d. To achieve the desired objectives of unified action and the synchronization and integration of military operations in time, space, and purpose, the JFC must consider many factors, some of which are:

(1) What objectives, when achieved, attain the desired end state?

(2) What sequence of actions is most likely to achieve the objectives?

(3) How can the resources of the joint force and interagency and multinational partners be applied to accomplish that sequence of actions?

(4) What is the likely cost or risk to the joint force in performing that sequence of actions?

e. The synergy achieved by integrating and synchronizing the actions and capabilities of conventional and unconventional forces jointly within the operational environment, enables the JFC to apply the force necessary to shock, disrupt, and defeat opponents.

*For additional information on multinational coordination see JP 3-16,* Multinational Operations.

# CHAPTER III
# AIR OPERATIONS

*"DOD leads military missions to deter, prevent, and defeat attacks on the United States, its population, and its defense critical infrastructure. This includes defending the maritime and air approaches to the United States and protecting US airspace, territorial seas, and territory from attacks…The bi-national North American Aerospace Defense Command (NORAD) is responsible for protecting the North American airspace over the United States and Canada. Aerospace warning and control are the cornerstones of the NORAD mission…"*

**Strategy for Homeland Defense and Civil Support**
**June 2005**

## 1. General

a. Since 9/11/01, significant changes in the conduct of aerospace defense have occurred in relation to the US homeland. To put these changes in context, it is important to understand the distinction between air defense and aerospace defense. The former is defined as "defensive measures designed to destroy attacking enemy aircraft or missiles in the atmosphere, or to nullify or reduce the effectiveness of such attack." The latter includes air defense, ballistic missile defense and the defense of US space assets. DOD, in partnership with NORAD, provides for the aerospace defense of the US homeland.

b. DOD is charged with defeating air threats to the United States, such as attacks from military aircraft and ballistic and cruise missiles. DOD must also be prepared to intercept nontraditional air threats, even when the intent to harm the United States is uncertain. These threats could include commercial or chartered aircraft, general aviation, ultralight aerial vehicles, unmanned aerial vehicles, radio controlled aircraft or even balloons. Early detection and successful interception of these types of potential threats require very close cooperation with DOD's interagency partners.

## 2. Air Operations in the Conduct of Homeland Defense

a. The combatant commanders with geographic HD responsibilities must consider the unique aspects of aerospace operations within the homeland. Figure III-1 highlights some of these considerations.

(1) **Size**. The AORs of the combatant commanders with geographic HD responsibilities include vast areas of airspace, land masses, and sea. North America in particular, is a huge land mass with multiple avenues of approach that an adversary could easily exploit to their advantage. To maintain an appropriate defense posture, the CCDRs are required to control the entire airspace over the approaches to and land masses within their AORs.

(2) **Control of Airspace**. DOD is responsible for defeating traditional and nontraditional aerospace threats to the United States. However, day-to-day US airspace is under the control of the FAA. Civilian control of airspace, as well as other functions vital to

the security of the homeland, makes it essential to coordinate with other government agencies.

(3) **Peacetime Environment.** Operations must be conducted in peacetime, as well as in times of crisis.

(4) **Duration**. Defense of the homeland is continuous. For example, Operation NOBLE EAGLE (ONE), involving US and Canadian air, land, and maritime forces is a 24/7 operation in peacetime as well as in times of crisis – it will continue for the foreseeable future - persistence is critical (ONE is discussed in detail, later in this chapter).

(5) **Rules of Engagement**. The airspace environment over areas of the homeland is dense – up to 5,000 aircraft at a given time over CONUS, for example. ONE operates with strict ROE in this very dense airspace environment. The ROE for operating in US airspace often produce a constrained engagement environment.

b. **SecDef has designated CDRNORAD as the supported commander for aerospace warning and aerospace control aspects of HD within the NORAD OA. The**

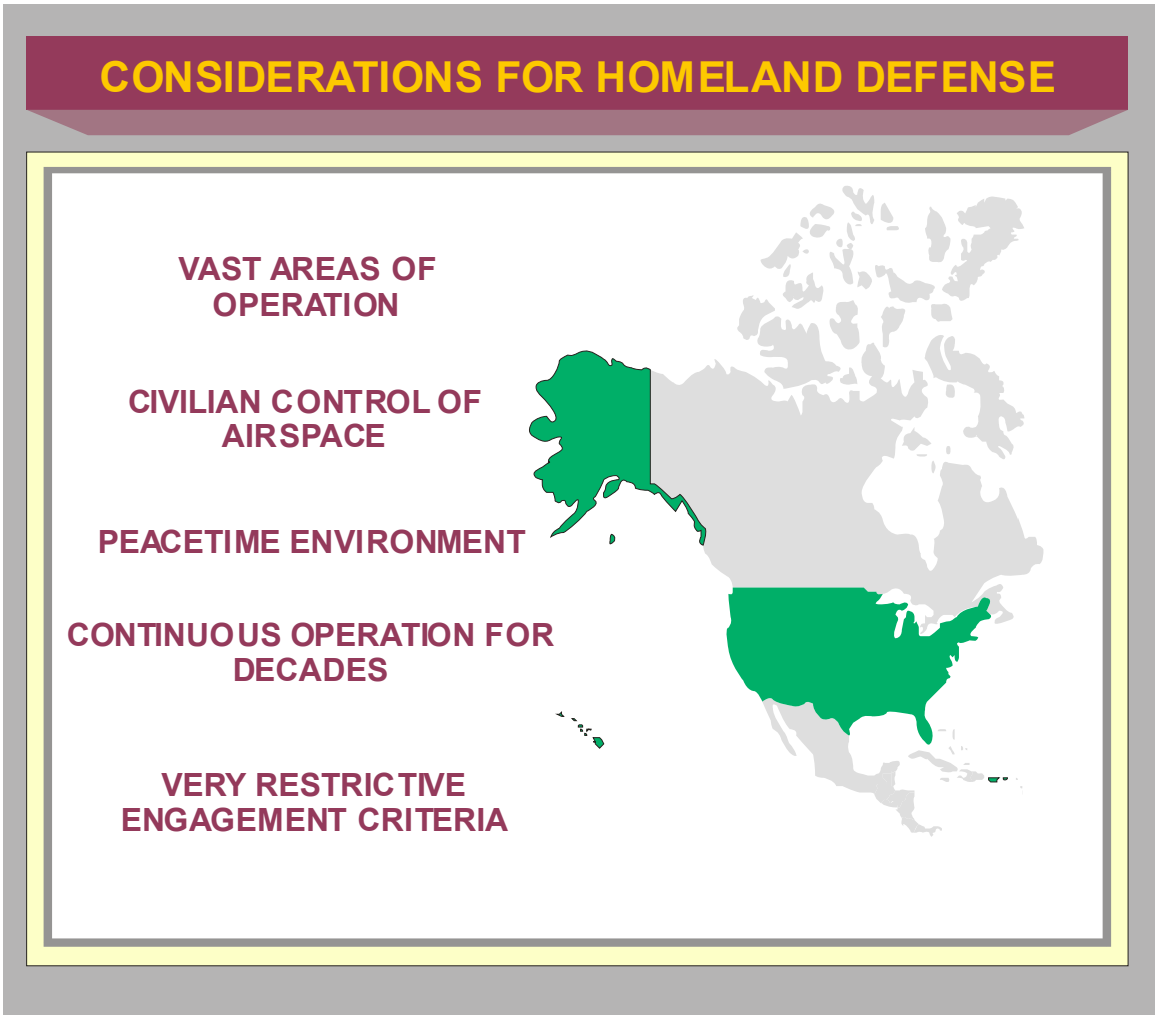



**Figure III-1. Considerations for Homeland Defense**

**OA includes the portions of the homeland that fall within the USNORTHCOM and USSOUTHCOM AORs, specifically CONUS, Alaska, the US Virgin Islands and Puerto Rico. CDRUSPACOM is the designated CCDR for HD missions within the USPACOM AOR. CDRUSNORTHCOM is the supported CCDR for HD missions within the USNORTHCOM AOR that are not under the direction of CDRNORAD**.

c. The missions of NORAD and USNORTHCOM are complementary. NORAD conducts missions and operations in the NORAD OA and provides warning of all airborne threats to include aircraft and missile attack and threats existing in the maritime domain. USNORTHCOM conducts US-only air, land, and maritime defense. The commands work side-by-side and coordinate on many issues. NORAD is the cornerstone of the US homeland air defense capability and is an integral part of an active layered defense that relies on the early warning of an emerging threat to quickly deploy and execute a decisive response. NORAD plays a critical role in the aerospace defense of Canada and HD of the United States by providing aerospace warning and aerospace control. Aerospace warning consists of surveillance, detection, validation and warning of an attack against North America, whether by aircraft, missiles or space vehicles. Aerospace control consists of air sovereignty and air defense operations within US and Canadian airspace.

*For a more complete description of the NORAD missions, organization and structure see* Appendix C, "North American Aerospace Defense Command, Missions, Organization, and Structure."

### 3. Homeland Air Defense

a. The President, through SecDef, directs DOD to conduct operations in defense of the US homeland, sovereign territory and national critical infrastructure (including DCI and other key assets, as required). DOD conducts homeland air defense using defensive counterair operations, which are comprised of active and passive air and missile defense.

(1) **Operation NOBLE EAGLE**. ONE is the overall umbrella operation covering HD for North America and Hawaii. As the binational, leading element of this operation, NORAD is tasked to support ONE by employing the forces and C2 necessary to protect North America from air attack. In Hawaii, USPACOM provides command and control (through Pacific Air Forces) with the Hawaii ANG providing ONE support. While providing a formidable deterrent in itself, it is important to emphasize that DOD and NORAD air defense capabilities represent the last line of air defense that will be used only if the other layers of overseas defense and domestic aviation security, conducted by civilian LEAs, have proven unsuccessful.

(a) NORAD forces maintain a steady state, quick response posture to counter potential threats to North America. NORAD conducts irregular air patrols above major metropolitan areas and critical infrastructure facilities, in addition to maintaining an alert force of fighter, tanker, and control aircraft. Aircraft sorties and alert commitments are based on a tiered response system. As threat levels intensify, the number of aircraft on alert

and on patrol increase. As the threat is evaluated, air patrol locations and frequencies are reviewed and updated.

(b) The US and Canadian governments have approved specific ROE to counter hostile acts within domestic airspace, which include expedited procedures and safeguards to account for the significant air traffic in domestic airspace.

(c) The authority and decision to engage is made at the highest levels of command. NORAD continues to refine its procedures and coordination with DHS; Public Safety and Emergency Preparedness Canada; the FAA and its Canadian equivalent, NAV CANADA; civilian law enforcement organizations and other government agencies within the United States and Canada.

*The ONE Tactics, Techniques and Procedures Reference Guide provides detailed mission planning and employment considerations for NORAD aerospace and land forces. It is designed to assist those involved in the tasking, planning and execution of ONE. This NORAD produced document also provides supplemental details to the areas discussed in Appendix C, "North American Aerospace Defense Command Missions, Organization, and Structure."*

(2) **National Capital Region - Integrated Air Defense System (NCR-IADS).** Because terrorists and other adversaries consider an attack on the NCR a continuing goal, it requires focused defense and security measures. DOD employs an integrated air defense system as part of the around-the-clock, multilayered, joint military and interagency effort. Figure III-2 provides a pictorial of the NCR-IADS components. The NCR-IADS augments the ONE fighter defenses by providing "assets in-place" in a quick reaction posture to protect the seat of the US government, as well as other key locations in the NCR, from air attacks.

(3) **Interagency Aviation Security Efforts**. Interagency roles, responsibilities, and required coordination protocols for conduct of aviation security and defense operations to counter threats to the US are contained in the AOTR Plan. TSA and other elements of DHS, as well as DOJ and DOT, conduct significant aviation security efforts throughout the United States and in the NCR. Principal among the efforts designed to improve interagency coordination is the National Capital Region Coordination Center (NCRCC), sponsored by TSA. The NCRCC enhances interagency coordination by providing a venue for representatives of the many organizations with a stake in the defense of the NCR to "stand watch" together. Through the NCRCC, various agencies have improved situational awareness of the actions of their defense partners. The NCRCC is a "coordination center" - no command or control of forces occurs. Participants include the FBI, TSA, FAA, US Capitol Police, US Secret Service, US Customs and Border Protection Office of Air and Marine Operations, USCG, JFHQ-NCR, and NORAD. Representatives from other state and local law enforcement agencies and the Joint Air Defense Operations Center also participate at the NCRCC when threats or circumstances warrant.

b. While not directly included in homeland air defense, offensive counterair (OCA) consisting of attack operations to include those on missile sites, airfields and C2 infrastructure conducted in foreign territory, ultimately supports a secure homeland by removing adversary capabilities before they can present themselves as a direct threat to the homeland. Extending beyond OCA, and part of the national security arsenal, are strategic attack operations which are aimed at affecting our adversaries' leadership, conflict-sustaining resources, and/or strategy. These attacks seek to weaken the adversary's ability or will to engage in conflict or continue an action and as such, could be part of a campaign, major operation, or conducted independently as directed by the President or SecDef. These

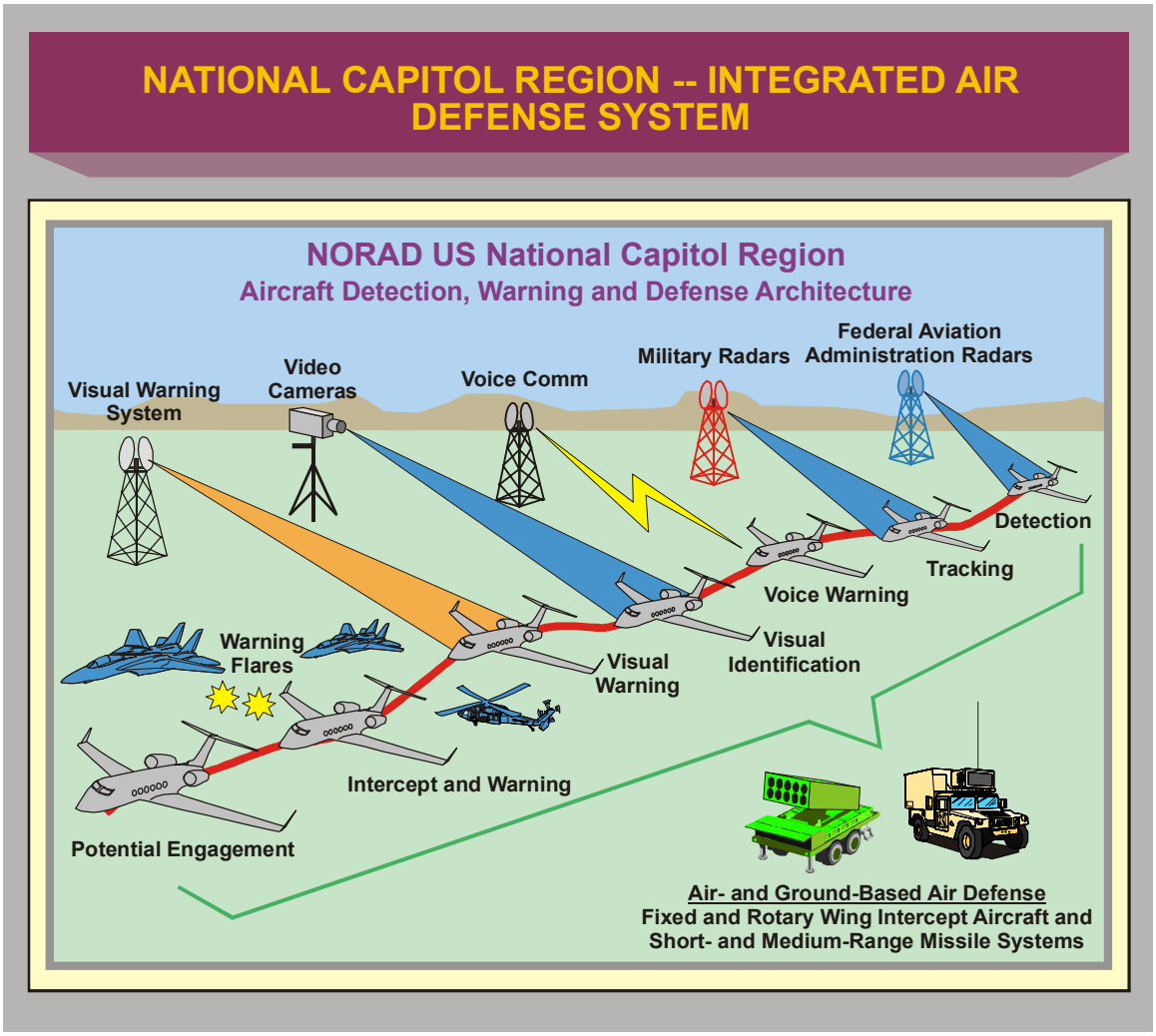



**Figure III-2. National Capital Region – Integrated Air Defense System**

attacks may directly or indirectly achieve strategic objectives without necessarily having to achieve operational objectives as a precondition.

c. Additional air defense assets may be employed in the United States when threat or circumstances warrant, including cruise missile defense assets. NORAD also has a role in missile defense to include HD against cruise missiles. USSTRATCOM has the

responsibility for planning, integrating and coordinating global missile defense operations and support.

*For more information on the full range of air operations consult the following doctrinal publications: JP 3-01,* Countering Air & Missile Threats; *JP 3-09.3,* Close Air Support; *JP 3-17*, Air Mobility Operations; *JP 3-30*, Command and Control for Joint Air Operations; *JP 3-52*, Airspace Control in a Combat Zone; and *JP 3-60,* Joint Targeting.

## 4. Aviation Security Policy

The US Aviation Security Policy (Homeland Security Presidential Directive [HSPD]-16/National Security Presidential Directive [NSPD]-47) directs USG departments and agencies to accomplish specific tasks that will continue the enhancement of HD and HS, by protecting the United States and US interests from threats in the air domain. Necessary actions to focus on include:

(1) Protection of critical transportation networks and infrastructure, from terrorist attacks or hostile acts, and reduce the vulnerability of the air domain to such acts or exploitation.

(2) Improving situational awareness of, and enhancing the sharing of information related to the air domain; improving early identification of threats and actions in response to those threats.

(3) Ensuring seamless, coordinated efforts relating to the security of the air domain among all relevant authorities.

(4) In the event of an attack, ensuring the resilience and recovery of the Aviation Transportation System.

(5) Countering the illicit acquisition and use of stand-off weapons systems that pose significant risks to the lawful civilian and military use of the air domain.

(6) Enhancing international relationships and advance common security interests in the air domain by promoting the integration of US allies and other partners into an improved global aviation transportation security framework.

# CHAPTER IV
## LAND OPERATIONS

*"We have learned that terrorist attacks are not caused by the use of strength; they are invited by the perception of weakness. And the surest way to avoid attacks on our own people is to engage the enemy where he lives and plans. We are fighting that enemy in Iraq and Afghanistan today so that we do not meet him again on our own streets, in our own cities."*

**President George W. Bush**
**September 7, 2003**

## 1. General

The threat to the homeland is difficult to predict and increasingly diverse. The likelihood of conventional large-scale land attack on the US may be remote, but the wide-range of threats that do exist must be addressed by land forces conducting HD. Historically, US land forces have concentrated on defeating threats as far away from the homeland as possible, and that remains the overarching goal. The central idea is to protect the homeland from external threats and aggression using integrated strategic, operational, and tactical defensive and offensive measures as the situation requires. The ability to detect, deter, prevent, or if necessary defeat land threats is a required capability for protection of the homeland.

a. Land operations conducted in support of HD require commanders to consider unique elements during planning and execution. More so than during traditional overseas military operations, HD operations require significant coordination and partnership between federal, state, tribal, and local government and agencies, especially since there is a significant overlap between DOD and law enforcement organization roles and functions. **This environment presents unique and complex operational challenges due to the necessity to achieve unity of effort within a Constitutional framework of sovereign states, and the need to be prepared to interface with a large number of disparate government agencies, IGOs, and NGOs**. For example, the Homeland Security Act of 2002 assigned the Secretary of Homeland Security the responsibility to prevent terrorists and instruments of terror from crossing our borders and our ports of entry. However, the Act did not confer any authority to the Secretary of Homeland Security to direct the engagement of DOD forces in offensive or defensive operations. As a result, the authority to direct DOD land forces remains with SecDef and the Armed Forces remain the key resource in conducting HD operations. Additional information on DHS is contained in Appendix A, "Transitioning Between Homeland Defense and Civil Support," and Appendix B, "Key Interagency Organizations."

b. Successful commanders coordinate with appropriate agencies to clearly define responsibilities and missions, leverage capabilities of AC and RC forces, and to ensure efficient and effective application of military forces in HD.

c. Military operations in support of HD also require a significant partnership between state- and federal-controlled forces. National Guard and reserve forces provide significant capabilities during planning and executing missions in defense of the homeland, as they

provide a military presence throughout the homeland with unique working relationships with state and local entities. Commanders leverage benefits and costs of AC, National Guard and reserve forces when planning operations. The RC is structured and operated to support assigned responsibilities as authorized, defined, and funded by the gaining AC. In that regard, the RC remains an integral part of total force power projection capabilities to respond to threats to the United States in all theaters of operation, to include those within the homeland. Moreover, the ability to use the NG for domestic operations has been enhanced by the addition of Chapter 9 to Title 32 USC which provides the capability to appropriately fund and leverage NG forces in this status for HD activities within the homeland. DOD planning for land operations in the conduct of HD appropriately integrates the employment of AC, NG and reserve forces to execute HD operations within the homeland. More detailed information on authorized NG statuses is provided in Appendix A, "Transitioning Between Homeland Defense and Civil Support."

## 2. Land Operations in the Conduct of Homeland Defense

a. The CCDRs with geographic HD responsibilities must anticipate, plan and be prepared for the possibility of land defense operations. HD land defense actions may include forcible entry from the land, sea, or air; decisive fires and maneuver; closing with and destroying a determined enemy; sustaining a joint force; and setting conditions for a return to peace. Specific defensive land operations in support of HD may include security operations through FP tasks or protection of critical defense infrastructure. Defensive land operations leverage existing federal agencies' capabilities (e.g., DHS).

b. Offensive operations take the battle to the enemy. This takes the initiative from the enemy, gaining freedom of action creating desired effects to achieve operational objectives. Follow-on forces deploy to expand the combat power established by initial entry forces. Although land defense forces may be required to defend in the short term, decisive results require shifting to the offense as soon as possible. However, HD operations should be of limited duration and conclude when the land forces achieve the objectives of the operation:

(1) Disrupt enemy coherence and dissipate his power.

(2) Secure or seize important terrain.

(3) Deny the enemy resources for continued hostile operations.

(4) Fix the enemy in place for destruction or capitulation.

(5) Gain information to support continuing operations against enemy forces.

c. As with other military operations, land operations in the conduct of HD are planned and executed by the CCDRs with geographic HD responsibilities, through their respective combatant commands, and their subordinate commands; either Service specific task force headquarters, JTFs, or a JFLCC. As with land operations in other theaters, commanders consider the scope of the operational environment, specified and implied tasks,

and span of control when selecting the appropriate C2 relationship. In addition, commanders consider the interagency environment; the effect of current operations on the civilian populace; and the role of the state, tribal, and local LEAs, when determining the type of headquarters organization necessary to execute HD operations. Based upon available forces, each CCDR with geographic HD responsibilities has identified subordinate commands that establish or source headquarters for HD operations.

## 3. US Northern Command Land Operations

a. CDRUSNORTHCOM may employ designated land component response forces from the Army or Marine Corps to deter, defend, and defeat threats or aggression within the AOR. Two Service component commanders, Commander, USARNORTH (CDUSRARNORTH) and Commander, Marine Corps Forces North (COMMARFORNORTH) may be organized as functional components and designated as joint force land component commanders. The ability to use or combine functional components, standing or ad hoc JTFs, and/or Service task forces, provides CDRUSNORTHCOM flexibility in selection of forces to address any HD event that may occur in his AOR.

(1) Figure IV-1 shows how land forces may be requested, provided, and employed to respond to a crisis requiring a rapid response. When directed by the President or SecDef to conduct HD operations, CDRUSNORTHCOM can consider several initial land force options, as part of the joint effort: employ a quick response force (QRF) or rapid response force (RRF), directly; employ a JTF with OPCON over a QRF or RRF; employ a JFLCC with OPCON over a QRF or RRF; or employ USARNORTH or MARFORNORTH as a single-Service headquarters with OPCON of a QRF or RRF. Based on his decision, the CDRUSNORTHCOM sends a request for forces (RFF) to the Joint Staff. Once the RFF is approved, force providers are directed to source personnel and equipment through Service components and provide them to CDRUSNORTHCOM. If a larger force is required, then follow-on forces can be employed. These follow-on forces may combine with the QRF or RRF as a task force, under a JTF.

(2) As the Army component command of USNORTHCOM, USARNORTH has two deployable task forces which serve as the permanent nucleus of JTFs that can be formed rapidly with augmentation. These task forces / JTFs provide C2 for Title 10 USC forces conducting HD missions. On order from CDRUSNORTHCOM, CDRUSARNORTH has the mission to serve as the JFLCC in HD operations, including QRF / RRF missions. CDRUSARNORTH, when designated a JTF commander, also has the ability to provide C2 for multiple JTFs as a JFC. Through continuous coordination with other Service components, federal, state, tribal, and local agencies including the NGB, state joint force headquarters, and Title 32 USC JTFs, CDRUSARNORTH plans and prepares for potential HD operations. CDRUSARNORTH also oversees the Army component DOD AT program and FP measures conducted in the USNORTHCOM AOR. Additionally, CDRUSARNORTH plans and implements the Army service component command portion of USNORTHCOM security cooperation activities undertaken with Mexico and Canada.

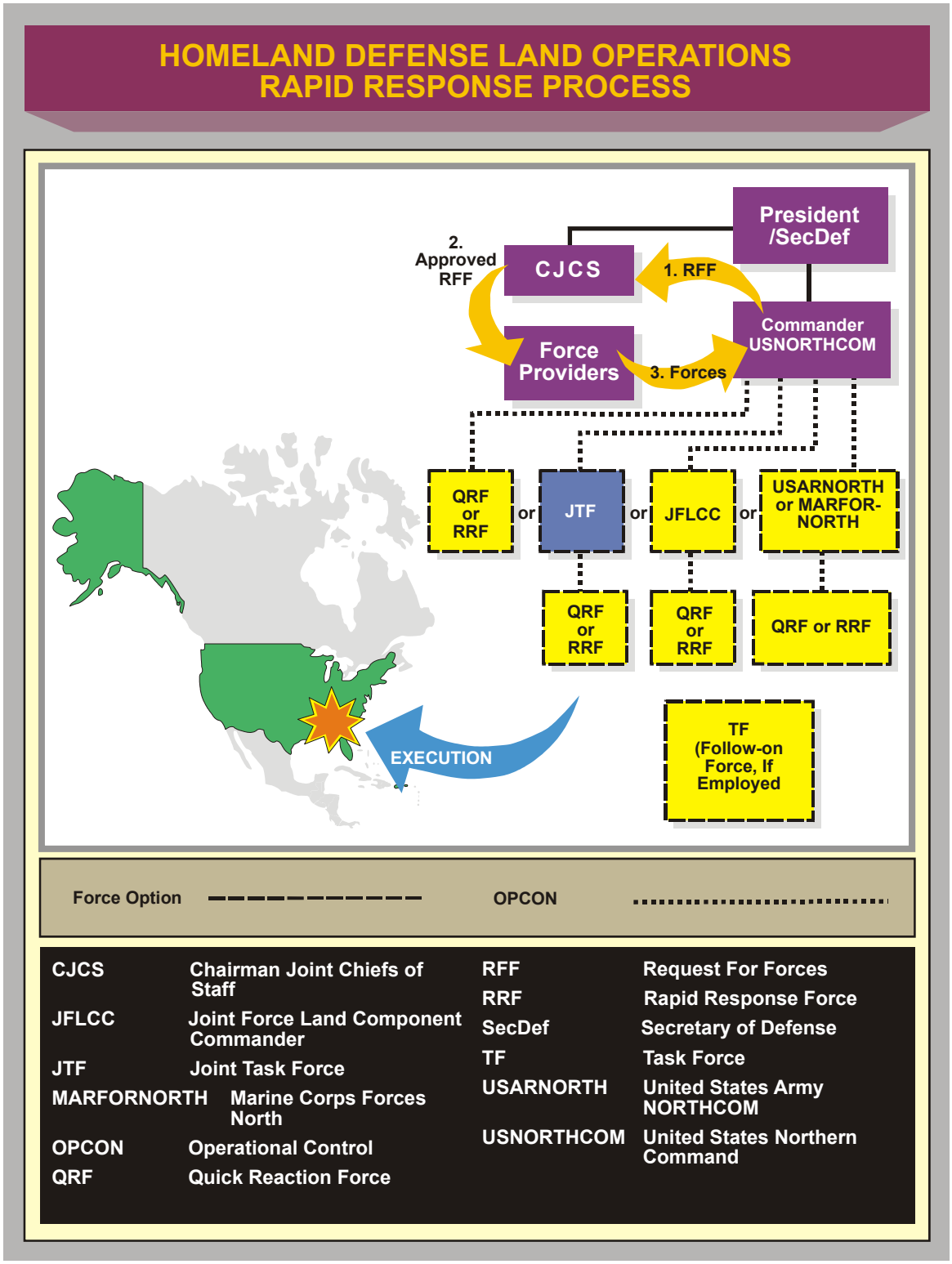



**Figure IV-1. Homeland Defense Land Operations Rapid Response Process**

(3) MARFORNORTH, has the ability to function as a JFLCC, with augmentation. Among the duties of COMMARFORNORTH are AT programs and FP responsibilities for Marine Corps installations. In addition to the command responsibilities,

COMMARFORNORTH supports, coordinates, and provides advice to CDRUSNORTHCOM on the employment of Marine forces when they are attached to USNORTHCOM in the conduct of HD operations.

b. Although considered extraordinary, conditions may arise that require conventional land operations within the continental limits of the United States (to include Alaska). In such instances forces will be made available to USNORTHCOM. These operations will be guided by established doctrine, principles and fundamentals. Procedures for identifying C2 structures, requesting and employing response forces, and coordinating actions will be consistent with established doctrine. Special considerations will likely apply due to the unique nature of operating in the homeland environment and requirement for DOD-wide and interagency coordination. Figure IV-2 illustrates how land forces may be organized to defend against a larger threat within the AOR requiring sustained operation with land forces. Conventional land forces are provided CDRUSNORTHCOM per the RFF process described above, and allocated to the JFLCC or the commander, JTF (CJTF) who has OPCON over these forces.

## 4. US Pacific Command Land Operations

a. CDRUSPACOM established Joint Task Force-Homeland Defense as the headquarters responsible for land HD operations on all bases and in all the US territories within the USPACOM AOR. CG USARPAC is dual hatted as the CDR JTF-HD. CDR JTF-HD provides trained and ready forces in support of security operations, from engagement to warfighting; these forces promote regional stability, and ensure successful crisis response and decisive victory. USPACOM also provides an Alaska-based QRF and RRF via JTF-AK, for employment by USNORTHCOM for HD operations in the Alaska JOA.

b. Along with being designated CDR JTF-HD, CG USARPAC is Commander, Task Force-Hawaii. Commander, US Navy Forces Marianas, Marianas Islands is designated Commander, Task Force-Guam under CDR JTF-HD. For land operations, and in coordination with civil authorities, these units are assigned the following tasks:

(1) Detect and dissuade attacks within their assigned operational area.

(2) Plan and conduct deterrence operations.

(3) Defeat threats within the assigned operational area.

(4) Employ forces to protect military installations and assigned critical infrastructure.

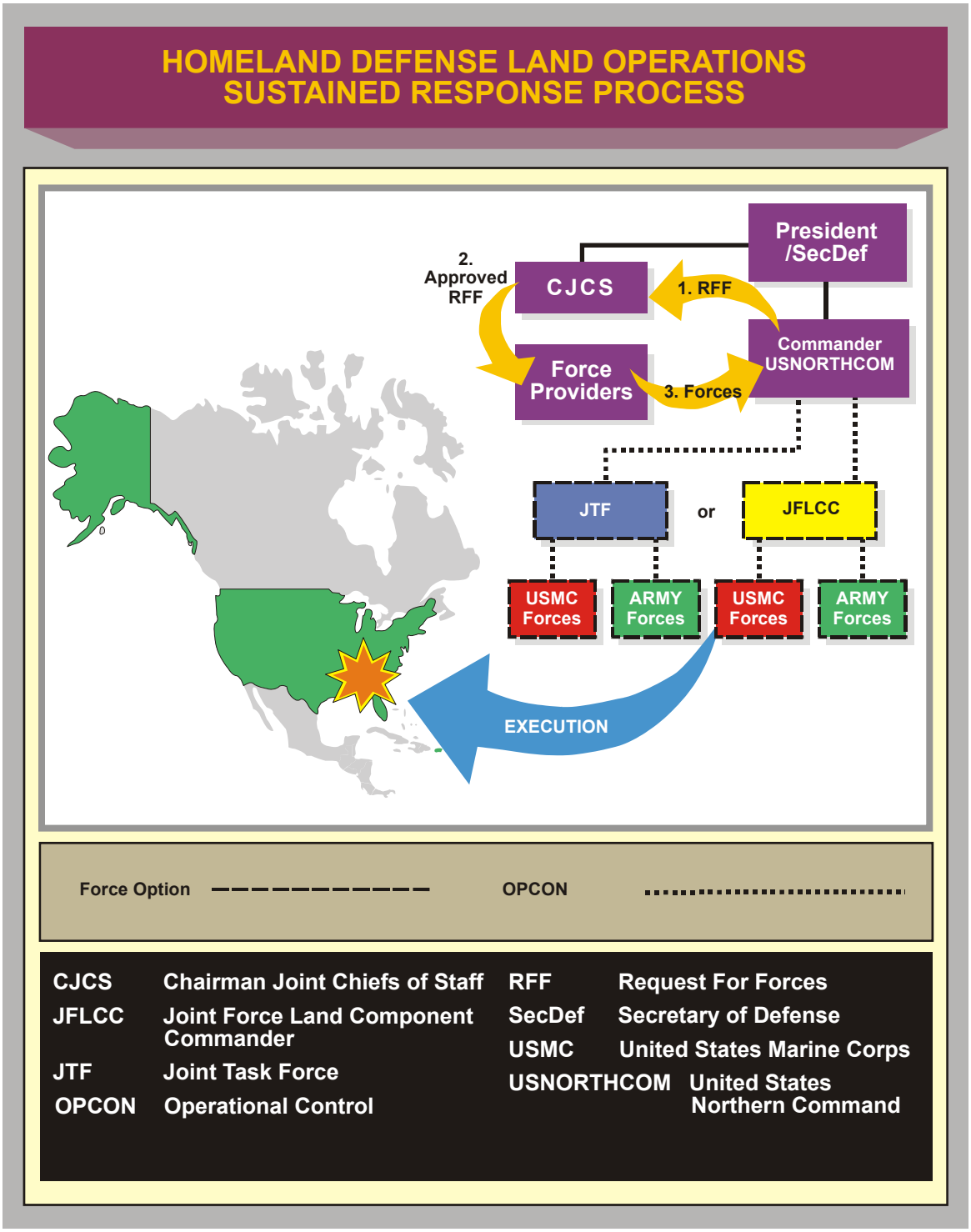



**Figure IV-2. Homeland Defense Land Operations Sustained Response Process**

## 5. US Southern Command Land Operations

a. USSOUTHCOM established USARSO to serve as the headquarters responsible for land HD operations in Puerto Rico and the US Virgin Islands. USARSO is the joint force land component and provides planning and C2 functions for operations in those regions. Other Service components, such as MARFORSOUTH may augment USARSO capabilities

by providing a special purpose Marine-air ground task force, as directed by CDRUSSOUTHCOM. Figure IV-3 shows this relationship.

b. The CAA between CDRUSNORTHCOM and CDRUSSOUTHCOM provides additional guidance regarding the defense of the homeland within the USSOUTHCOM AOR.

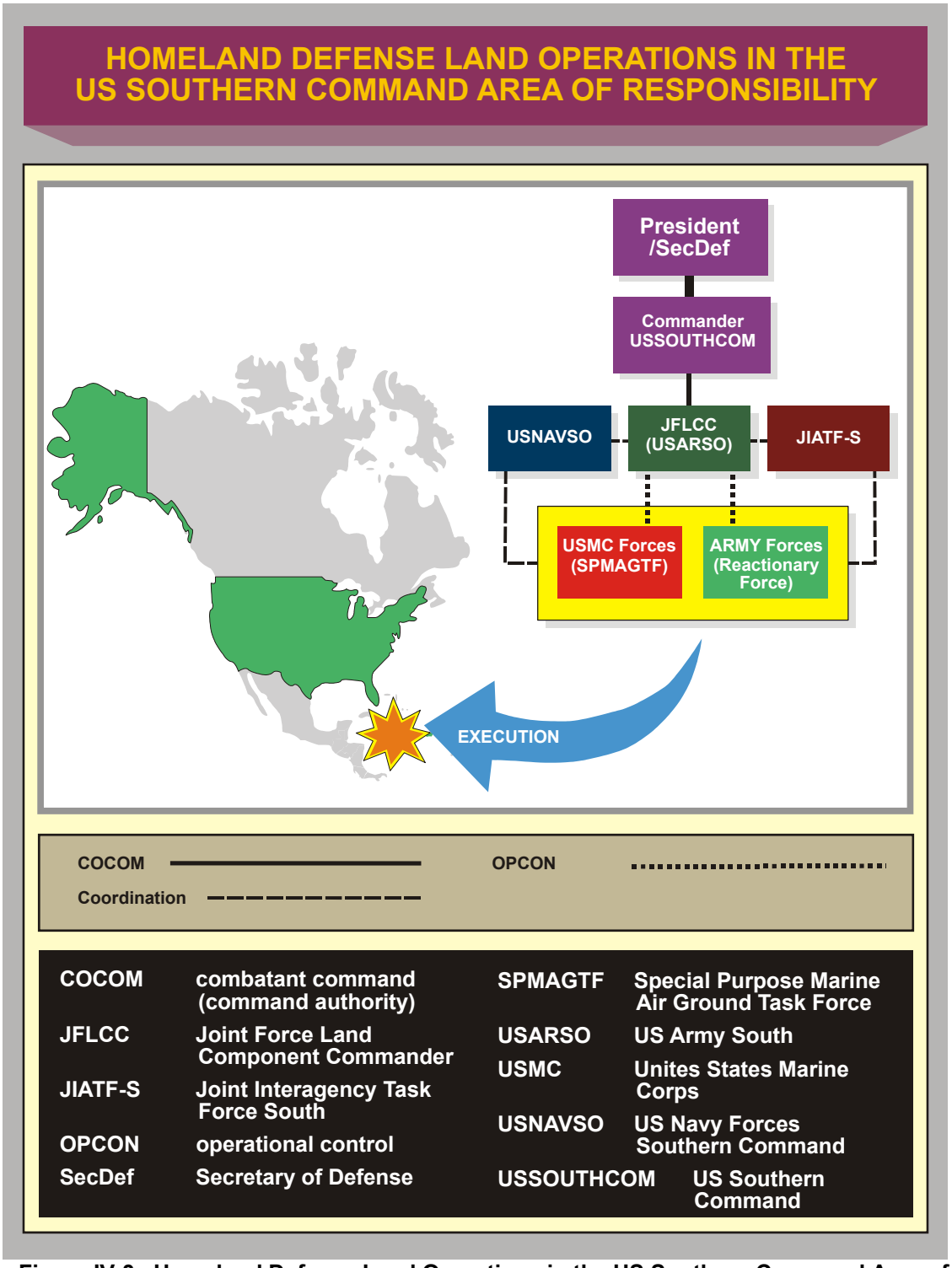



**Figure IV-3. Homeland Defense Land Operations in the US Southern Command Area of Responsibility**

Intentionally Blank

# CHAPTER V
# MARITIME OPERATIONS

*"It is the policy of the US to take all necessary and appropriate actions, consistent with US law, treaties, and other international agreements to which the United States is a party, and customary international law as determined for the United States by the President, to enhance the security of and protect US interests in the maritime domain"*

**President George W. Bush**
**December 21, 2004**

## 1. General

a. Securing the maritime approaches is essential to keeping the homeland safe. DOD maritime assets must be able to detect, identify, localize, evaluate, sort, and when warranted, intercept or interdict to prevent or defeat an attack. This is a complex task as adversaries may not be easily differentiated from normal maritime activity, and any disruption of commercial trade may have economic and financial implications domestically and internationally. It is also critical for DOD to maintain unrestricted freedom of movement to ensure the ability to deploy forces overseas.

b. In this dynamic environment, responding to these unpredictable and transnational threats requires coordination across the USG to prevent attacks on the homeland. Coordination and interoperability with federal, state, tribal, and local LEAs, particularly the USCG, Customs Border Protection, and FBI, are important in this effort due to overlapping authorities, responsibilities and potential simultaneous presence of response assets for maritime operations in the conduct of HD. Additionally, sharing of information and cooperation with allied nations in regards to global maritime activities will greatly assist in the early detection and subsequent interception of maritime threats.

## 2. Maritime Operations in the Conduct of Homeland Defense

a. DOD, through the relevant CCDR, is prepared to respond to maritime threats from the forward regions to the homeland. DOD maritime forces support an active layered defense through extensive operations in the forward regions, coupled with a high state of readiness and scalability to varying threat conditions in the maritime approaches and homeland. DOD plays the lead role in a maritime HD construct, where DOD is identified as the federal agency with lead responsibility whether it is by discovery of a threat during normal operations, which requires immediate action, or through the protocols established by the MOTR Plan. These protocols are based on existing law, desired USG outcome, greatest potential magnitude of the threat, response capabilities required, asset availability, and authority to act. In the HD construct, USCG assets may also come under the control of the US Navy (USN) to defeat the threat to the United States. Conversely, if it is determined to be a DHS mission, DOD assets could come under TACON of the USCG.

b. *The National Strategy for Maritime Security (NSMS)* and the MOTR Plan are directed in the NSPD-41/HSPD-13, *Maritime Security Policy*. The MOTR Plan operationalizes NSPD-41/HSPD-13 and the NSMS by achieving a coordinated USG response to a vast array of threats in the maritime domain, including:

(1) Nation-state military threats.

(2) Piracy.

(3) State/non-state criminal, unlawful or hostile acts such as smuggling and WMD proliferation activities.

(4) Threat vessels with cargo and/or personnel requiring investigation and disposition.

c. The MOTR plan predesignates federal agencies with lead responsibilities, clarifies interagency roles and responsibilities, and establishes protocols and procedures that are utilized for a coordinated response to achieve the USG's desired outcome for a particular threat. The MOTR predesignated leads were developed from the following criteria:

(1) USG desired outcome.

(2) Agency authorities.

(3) Agency capabilities.

(4) Agency asset availability.

(5) Magnitude of the threat.

(6) Existing law.

d. The MOTR protocols and procedures allow rapid response to short-notice (pop-up) threats and require interagency partners to begin coordination activities (i.e., MOTR conference calls) at the earliest possible opportunity when one of the following triggers are met:

(1) Any specific terrorist or state threat exists and US agency response action is or could be imminent.

(2) More than one federal department or agency has become substantially involved in responding to the threat.

(3) The agency or department either lacks the capability, capacity, or jurisdiction to address the threat.

(4) Upon resolving the threat, the initial responding federal department or agency cannot execute the disposition of cargo, people, or vessels acting under its own authority.

(5) The threat poses a potential adverse effect on the foreign affairs of the United States.

e. The MOTR coordination process is conducted through a virtual network of interagency national and operational command centers. This coordination process is the key element in determining which agency is the right choice for leading the USG response and what other agencies are needed to support the response effort. Additionally, the MOTR protocols include a process for transition of the lead from one agency to another and dispute resolution (i.e., if the USG desired outcome cannot be resolved at the lower levels of government, the characterization of a particular threat could ultimately be elevated for resolution by higher authority). At the tactical level, it is important to realize that the MOTR process exists not only to achieve a USG desired outcome, but to coordinate and assist in bringing additional capabilities to bear on a threat.

f. Additionally, MOTR presents guiding principles that apply to all agencies at all times and sets the basic standards for interagency actions to overcome maritime threats to the United States:

(1) The USG takes all necessary steps to prevent terrorist attacks, WMD from entering the United States, its territories, and possessions; and catastrophic disruption of normal activities in the maritime domain.

(2) USG agencies are prepared to conduct MOTR quickly and decisively to intercept, apprehend, exploit, and, when necessary, defeat maritime threats.

(3) Any MOTR agency shall take those actions necessary to defeat a threat that presents an imminent risk of death, serious physical injury, or substantial destruction of property, consistent with the law and the rules on the use of force, including the use of lethal force.

g. Successful MOTR execution is fundamentally reliant on the operational-intelligence linkage. This linkage is optimized through ongoing efforts to achieve maritime domain awareness. Maritime domain awareness seeks to provide the requisite intelligence and information that facilitates timely decision making. The goal is to identify threats as early and as distant from the homeland as possible, but no later than to allow time to defeat or otherwise overcome threats at a safe distance from the US. This is accomplished through the effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy, or environment of the US. Maritime domain awareness improvement efforts are guided by two NSMS supporting plans (i.e., Plan to Achieve Maritime Domain Awareness and the Global Maritime Intelligence Integration Plan).

*For additional information on maritime domain awareness, refer to JP 3-32*, Command and Control for Joint Maritime Operations.

h. DOD or USCG assets operating under Title 10 USC, under the control of the CCDR, maintain the ability to conduct a range of options against suspect ships and vessels in the maritime approaches to and the territorial waters of the United States. While USN ships and aircraft are conducting training in home waters prior to overseas deployments, they are rapidly scaleable for HD operations or to support other federal agencies should the situation dictate. These options range from surveillance and tracking, to maritime interception (MIO), including the application of lethal and nonlethal force if necessary.

### 3. Joint Force Maritime Component Operations

a. The JFMCC plans and executes operations in the maritime domain while supporting the operations of the other components as directed. COMUSFLTFORCOM is designated as JFMCC North for CDRUSNORTHCOM and supports and is supported by the USCG in the USNORTHCOM AOR. COMPACFLT is designated the JFMCC for CDRUSPACOM, supports the USNORTHCOM JFMCC for HD, and supports and is supported by the USCG in the USPACOM AOR. Commander USNAVSO provides the JFMCC for CDRUSSOUTHCOM, support to USNORTHCOM JFMCC for HD, and support to and is supported by the USCG in the USSOUTHCOM AOR. Additionally, CDRNORAD's maritime warning mission supports HD operations as defined in the NORAD Agreement and Terms of Reference.

b. **JFMCC Mission:** JFMCC planning must be in consonance with the guidance of senior commanders, must support the JFC concept of operations, and should support other component commanders as well. The JFMCC's operational concept is typically built upon the following strategic missions:

(1) Sea control.

(2) Maritime power projection and projection of defense from sea to land.

(3) Deterrence.

(4) Strategic sealift.

(5) Forward maritime presence.

(6) Seabasing operations.

(7) Other specified and implied tasks in the execution of HD can involve planning and directing naval operations (e.g., undersea operations, mine operations, strike operations, fires, interdiction, amphibious and expeditionary operations, and MIO), as well as providing communications systems support and FP.

*For further information, see* JP 3-32, Command and Control for Joint Maritime Operations.

c. Maritime HD operations may be accomplished independently or in support of other operations. When established, a maritime AO can include international and territorial waters, harbor approaches, ports, waterfront facilities, and those internal waters and rivers that provide access to port facilities (including associated airspace). The JFMCC plans and conducts HD operations to maintain sea control; strengthen port security and/or harbor defense (PS/HD) and harbor approach defense; ensure strategic mobility; provide a secure environment for US and coalition forces; and support other component commanders, as directed.

(1) The JFMCC ensures any supporting forces are properly integrated into the maritime plan, which in turn is integrated into the overall plan.

(2) The CCDR should establish corresponding relationships with the JFMCC and other components to coordinate security operations. For especially critical facilities, dedicated defense forces such as Marine Corps security forces, Air Force security forces, and Army military forces may be in the maritime AO, along with the Navy Shore Patrol and USCG security forces.

(3) Close liaison between the JFMCC and appropriate host nation, federal, state, tribal, and local agencies is necessary to effectively operate in the forward regions, approaches and within US territorial waters. During many types of maritime operations, civilian cooperation forms an important element of logistics, intelligence, and FP planning. Liaison with the standing area maritime security committees is a way to acquire support and coordination.

(4) The need to liaise extends to foreign and coalition countries and IGOs; and must take into consideration international agreements such as the Canada-US Rush-Baggot Treaty which impacts upon operations on the Great Lakes and Saint Lawrence seaway system.

## 4. United States Navy and United States Coast Guard Relationships

a. USCG authorities are vested in both Title 10 USC, as a branch of the Armed Forces of the United States, and Title 14 USC for federal law enforcement and other duties. A close alliance of US maritime forces is increasingly crucial to contend with challenges to US sovereignty and maritime HD that continually grow more diverse and complex. Continuous USN and USCG teamwork across the spectrum of maritime operations provides a strong foundation for dealing effectively with emerging challenges that include the global war on terrorism, regional conflict, crisis response, sanctions enforcement, arms trafficking, weapons proliferation, mass migration, smuggling, natural resource depletion, and FP.

b. The USCG's military readiness responsibility is complemented by a broad array of ongoing maritime missions and authorities (Title 14 USC) that include law enforcement; maritime threat response and advanced interdiction boardings; marine safety; ports, waterways and coastal security; search and rescue; aids to navigation; illegal drug and undocumented migrant interdiction; and defense readiness among others. These USCG core competencies include resources and capabilities that contribute significantly to HD.

c. During HD operations, the employment of maritime forces is governed by specific tasks in plans or orders. A USCG captain of the port (COTP) will normally be responsible for harbor control within the port while the JFMCC is responsible at sea for maritime communications, surveillance, detection, maritime interdiction and interception operations, protection of high value assets (HVAs), and the enforcement of exclusionary zones.

d. Each USCG COTP has legislative mandates and authorities for the safety and security of US ports including safeguarding harbors, vessels, and waterfront facilities from accidents, negligence, terrorism, sabotage, espionage, and other subversive acts. Port safety is focused on preventing accidental damage to vessels and port facilities through activities such as inspection, hazardous materials loading supervision, waterways management, and cargo transfer monitoring. Port security is usually carried out using law enforcement authorities. Port safety and security are closely related, mutually supportive, and are often conducted concurrently. In the United States, maritime port security operations supporting military missions are likely to be focused on the seaports of embarkation (SPOEs) and high-value unit escorts. USCG support to military outload operations involves all port safety and security activities related to port facilities and vessels involved with the movement of military essential cargos at SPOEs. The USCG also has the capability to carry out these port security missions at seaports of debarkation (PODs) established by GCCs.

e. The USCG is an integral force for maritime HD mission execution. USCG statutory authorities remain in effect at all times, including when USCG forces are transferred to DOD control to execute maritime HD operations. When USCG forces conducting maritime HD operations under DOD control are needed to exercise specific USCG authority, the appropriate USCG commander must ensure that a USCG chain of command is reestablished. Maritime HD C2 structure is pursuant to the "*Memorandum of Agreement between the Department of Defense and the Department of Homeland Security for the Inclusion of the US Coast Guard in Support of Maritime Homeland Defense*."

f. The USCG's core competencies (both Title 10 USC and Title 14 USC responsibilities) in high seas interdictions, waterways management, littoral operations, and law enforcement complement USN operations and enhance the USG's ability to conduct unrestricted maritime operations worldwide. USCG forces may be used to support operations to include MIO to screen vessels for contraband (including terrorist and terrorist related materials), PS/HD, military environmental response to limit the potential

disruption to military operations by intentional marine pollution incidents that could occur in the AO, peacetime military engagement, and coastal sea control operations in the littorals to ensure the unimpeded use of designated offshore coastal areas by friendly forces and to deny the use of those areas to enemy forces. These operations can be conducted either independent of or in conjunction with a maritime HD operation.

## 5. Maritime Operations Requiring Interagency Coordination

Maritime operations in support of HD that require a coordinated government (federal, state, tribal, local) effort range from protection of ports, harbor approach defense, and countermine and mine countermeasures (MCM) operations to littoral, boarding, and MIO.

a. **Protection of Ports.** The harbor approaches will often be filled with shipping that is neither clearly friendly nor hostile. Most of these ships will have legitimate business in the port, and denying them entry may cause significant economic harm to the United States and possibly other countries as well. They must be cleared to ensure that they will not cause harm, intentional or unintentional, to the port.

(1) **Approaches**. USN and USCG units may challenge and clear suspect ships in the approaches before they enter port. These units are capable of remaining underway for weeks at a time and ensure that problems are defused before suspect maritime shipping is close enough to present a threat to the homeland (e.g., port). Once suspect maritime shipping is screened and is cleared to enter the port by the COTP, maritime forces may be used to escort the ship and provide security in and near the mouth of the harbor.

(2) **Harbor Approach Defense**

(a) Harbor approach defense involves the employment of maritime forces (surface and air) to conduct coastal sea control by tracking, identifying, and interdicting if necessary maritime threats within the designated defensive sea area (DSA). Harbor approach defense operations are an extension of PS/HD operations into the littoral and are normally conducted by USN and USCG units trained in MIO and capable of remaining dozens of miles offshore for weeks at a time, operating day and night in all weather. This area normally extends well beyond territorial waters to ensure that timely intercepts of inbound maritime shipping are made; boarding is completed prior to port entry to minimize commerce disruption; and to ensure that WMD remain well outside the homeland.

(b) Harbor approach defense operations are overt and defensive in nature, conducted primarily by units operating in littoral waters and include the following activities:

1. Show an overt harbor approach presence by conducting area patrols, to deter or preempt attacks.

2. Investigate and intercept inbound shipping, ensuring that all or some are boarded and searched for hazards that might intentionally (or unintentionally) pose a hazard to the port, while protecting outbound shipping.

3. Extend visual and sensor detection and intelligence collection capabilities.

4. Provide an immediate armed response upon seaward threat detection or classification.

(3) **Harbor Defense**. Harbor defense is the defense of a harbor or anchorage and its water approaches against external threats such as submarines, submarine-borne, or small surface craft attack; enemy minelaying operations; and sabotage (the defense of a harbor from guided missiles while such missiles are airborne is considered to be a part of air defense). It involves the employment of forces for the protection and management of harbors, ports, anchorages, shore facilities, and commercial, private, and naval vessels against waterborne and landward threats. DOD activities within the port or harbor are executed in close coordination with the COTP. In the port environment, the COTP, senior installation commander, and JFMCC will determine the appropriate assignment of maritime security and defense tasks based on threat conditions and necessary authorities, force capabilities, and availability. DOD forces generally remain under the C2 of DOD commanders for these activities. Coordination amongst federal, state, tribal, and local law enforcement and DOD forces both pier side and on the water is necessary. Thorough planning centered around the area maritime committee forum and IAW MOTR plan fundamentals provides a basis for unity of effort. The JFC, may form PS/HD units to support area defense efforts, if response time and forces are available. The JFC may appoint the harbor defense commander (HDC). The COTP when acting as the HDC normally sets the boundaries for harbor defense. Defense of the harbor is the responsibility of the HDC. The JFC may assign sub area operational commanders as needed for coastal sea control and harbor defense to conduct operations.

(4) **Port Security.** Port security missions involve the protection of designated marine terminals, pier areas, HVAs (including escorts while transiting into and out of ports or harbors), and other designated facilities. These missions are conducted for the safeguarding of vessels, harbors, ports, waterfront facilities, and cargo from internal threats such as destruction, loss, or injury from sabotage or other subversive acts; accident; thefts; or other causes of a similar nature. They also include port safety, marine environmental protection, waterway management, and search and rescue.

b. **Countermining and Mine Countermeasures Operations**

(1) Mining of homeland waters by enemies can be conducted by a variety of methods from surface vessels, air, submarines, or swimmers and/or divers. The objective of countermining is to prevent mining. Detection of such activity should be a priority for maritime surveillance systems monitoring the seaward approaches and internal waterways. Consistent with the MOTR Plan, DHS is the agency with lead responsibility for prevention

and detection of mining within waters subject to US jurisdiction. MCM operations can be conducted for the following reasons:

(a) Bottom mapping for operational environment awareness prior to an event.

(b) Exploratory operations to identify suspected mine threat and/or boundary of the threat area.

(c) Clearance operations to locate, identify, and neutralize mine threats.

(2) The support maritime forces may provide to MCM operations consists of protection for MCM assets and logistic support for ashore staging areas in the AO. Maritime forces provide air and surface patrol craft to enforce a security zone encompassing the MCM operational area, to protect MCM forces from harassment or attack.

(3) Logistic support to MCM forces is limited to messing, berthing, and potable water supplies. In the event that logistic support is required, consideration should be given to basing MCM assets with or adjacent to maritime forces to economize security and logistic support.

*For further information, see JP 3-15,* Barriers, Obstacles, and Mine Warfare for Joint Operations.

c. **Littoral Operations**

(1) Maritime security in the littoral region is attained through the use of a DSA where forces are employed to ensure the unimpeded use of designated offshore coastal areas by friendly forces and to deny the use of those areas to enemy forces.

(2) The conduct of maritime HD is the responsibility of the cognizant CCDR, which is CDRUSNORTHCOM for CONUS and Alaska; CDRUSPACOM for Hawaii, the US territories and possessions, and Freely Associated States located in the Pacific AOR; and CDRUSSOUTHCOM for Pueto Rico and US Virgin Islands. When directed by the President, responsibility for harbor defense, harbor approach defense, and sea control in the US littoral is shared between the USN and the USCG.

d. **Sea Lines of Communications/Chokepoint Operations.** Seaward security is a focused maritime operation that complements broader maritime operations designed to maintain sea lines of communications. The primary objective is to provide for the safe passage of strategic sealift and commerce to and from deep water and to deny use of these areas to enemy forces. Similarly, maritime forces can be employed in a chokepoint (e.g., narrow strait or canal) to provide for the safe passage of friendly forces through that chokepoint. Maritime units can be employed as part of a force—air, surface, and submarine units and their supporting systems, positioned across the likely courses of expected enemy transit—for early detection and rapid warning, blocking, and destruction of the enemy.

e. **Boarding Operations**

(1) Uncertainty and a need to verify status and cargo, or suspicions about the intentions of a crew or its ability to inflict damage/harm should never be discounted and often leads to a decision to inspect a vessel. Patrol craft must increase surveillance of the vessel during approach and throughout the inspection. Similarly, all weapons and equipment must be readied for immediate emergency action. Mounted weapons should be manned and armed, and personnel briefed per the SROE and/or SRUF.

(2) Boarding teams may be employed either at sea or in port to stop and/or gain control of a noncompliant vessel, gather intelligence, detain suspect personnel or seize illegal cargo. The teams employ specific techniques and procedures during a boarding. Boarding team members must understand the systematic and proven techniques to conduct searches for contraband.

*For further reference see, NTTP 3-07.11/Coast Guard Publication (CGP) 3-07.11,* Maritime Interception Operations.

(3) **Maritime Interception Operations (MIO)**

(a) MIO are designed to halt the movement of designated items into or out of a nation or area. Units involved in MIO not only provide unit presence but may also use reasonable force if a vessel is noncompliant. Each MIO varies from the next. The specific political, geographic, and tactical factors and the legal authority on which the MIO is based influence the enforcement procedures.

(b) MIO is a USN core competency. Many USN ships are capable of conducting compliant and certain types of noncompliant boardings. Maritime forces may also be tasked to conduct expanded MIO (EMIO). EMIO is authorized by the President through the SecDef to deter, degrade, disrupt, or prevent attacks against the US and its allies. EMIO involves interception of targeted personnel or materiel that possess an imminent threat to the US and its allies. EMIO may be implemented without sanctions and may involve multinational forces. USN ships must be augmented by other forces (e.g., Navy Seals or special operations capable Marines) to conduct high freeboard noncompliant boardings or to conduct opposed boardings against adversaries actively trying to escape capture.

(4) Boarding teams will be trained to board and search vessels in order to locate and defeat threats to the homeland. In addition, boarding teams must be sensitive to the tactical exploitation of evidence and personnel (e.g., proper identification, collection and protection of evidence; proper handling and custody of contraband, equipment, crew or other evidence found during an inspection; and training, planning and exercising intelligence collection and investigative techniques with LEAs). Boarding teams should anticipate augmentation by interagency, state, or local agency experts to deal with special situations such as WMD, immigration, etc.

(5) **Legal Authority**

(a) Individuals in positions of leadership must understand applicable legal authorities for all boarding operations. Specific guidance is issued by the chain of command for all operating areas and scenarios to further define requirements and guide boarding actions. Military requirements or US laws will often guide the chain of command in providing direction regarding specific action to be taken or specific conduct of the inspection. All team members must understand enforcement action requirements so that the inspection is conducted appropriately.

(b) All actions undertaken by the United States must be in accordance with legal guidance provided by the chain of command.

## 6. Employment of Fires

a. The range of lethal options available to maritime forces is significant. A limited number of nonlethal options exist, as well. Maritime forces can be employed to rapidly destroy, raid, or neutralize terrorist threats both at sea and ashore given actionable intelligence.

b. Maritime threats to the homeland may be presented in a variety of forms. From large cargo ships to fishing vessels, from cruise ships to pleasure craft. Once a vessel has been identified as a threat to the homeland, traditional anti-surface warfare options may be employed to disrupt, delay, disable or destroy the delivery of the weapons, cargo or people to its intended target. Naval forces may take action as defined by the chain of command and the SROE and supplementary measures, if any.

c. Depending on the threat, maritime HD options may be determined through the MOTR protocol process. Within the USNORTHCOM AOR, JFMCC NORTH will direct maritime HD operations that may include appropriate Service forces, USCG, or SOF to disrupt, delay, disable or destroy threat vessels.

Intentionally Blank

# CHAPTER VI
## SPACE OPERATIONS

*"Today's national security depends more than ever on capabilities that can only be delivered from space; the only place we can achieve the degree of global situational awareness needed by the intelligence community and the Department of Defense."*

**Dr. Donald M. Kerr**
**Director, National Reconnaissance Office**
**March 16, 2006**

## 1. General

The region of space above the United States cannot be owned or possessed like territory. It is USG policy, however, that purposeful interference with US space systems will be viewed as an infringement on the Nation's sovereign rights. In order to deter or preempt attacks and to protect military space assets, DOD conducts space operations in support of HD in the space control, space support, space force enhancement, and space force application areas. DOD DCI activities may be closely related to military space operations, given that selected space capabilities may be classified as DCI. These activities may serve to protect and defend our ability to operate in and through space. CDRUSSTRATCOM is the supported commander for protecting and defending the right to operate in space and is responsible for identifying, assessing, and securing DOD critical assets in space.

## 2. Space Operations in the Conduct of Homeland Defense

Military space operations bring enabling information to the JFC. For example, initial threat detections and location, global communication, real-time weather, high-resolution imagery and signals intelligence helps the JFC determine the appropriate intercept vehicle, location and/or time of attack. Using the global communication capability, the JFC is able to exercise real-time C2 functions and post-mission assessment. Satellite communications (SATCOM) technology can link HD forces with interagency, intergovernmental, and other federal and state, tribal, and local partners in support of HD operations. In addition, Global Positioning System (GPS), SATCOM, and geospatial information and services are available to track incoming threats from air, land, sea, or space. Information from space provides decision makers advance warning to prepare for, respond to, recover from, and prevent threats to the homeland.

a. Roles and Responsibilities

(1) CDRUSSTRATCOM is responsible for developing desired characteristics and capabilities, advocating, planning, and conducting space operations (force enhancement, space control, and space support, including space lift and on-orbit operations and force application). These responsibilities include:

(a) Providing warning and assessment of space attack.

(b) Supporting NORAD by providing the missile warning and space surveillance necessary to fulfill the US commitment to the NORAD Agreement.

(c) Serving as the single point of contact for military space operational matters, except as otherwise directed.

(d) Providing military representation to US national agencies, commercial entities, and international agencies for matters related to military space operations. This will be as directed and in coordination with the CJCS and other combatant commanders.

(e) Coordinating and conducting space campaign planning.

(f) Serving as the DOD Manager for Manned Space Flight Support Operations.

(2) CCDRs with geographic HD responsibilities have specific responsibilities for HD and are the supported commanders responsible for conducting HD operations within their respective AORs:

(a) Communicate space capability requirements to USSTRATCOM when acting in an HD capacity.

(b) Provide FP for space assets located within their respective AORs.

b. **Space Mission Areas**. There are four primary space mission areas, each providing necessary contribution to HD operations. The mission areas are: space control, space support, space force enhancement, and space force application.

(1) Space control operations provide freedom of action in space for friendly forces while, when directed, denying it to an adversary, and include the broad aspect of protection of US and US allied space systems and negation of adversary space systems. Space control operations encompass all elements of the space defense mission. Space control may involve activities conducted by air, land, maritime, and space forces and/or SOF. To gain space superiority, space forces must surveil space and terrestrial areas of interest that could impact space activities, protect the ability to use space, prevent adversaries from exploiting US, allied, or neutral space services, and negate the ability of adversaries to exploit space capabilities. These forces would be brought to bear against space systems or facilities identified through the targeting process. Space control operations will provide freedom of action in space for friendly forces and, when directed, deny the same freedom to the adversary. They include offensive and defensive operations by friendly forces to gain and maintain space superiority and situational awareness of events that impact space operations. HD planners should consider protection of space and ground support assets within the AORs of the CCDRs with HD responsibility, when drafting FP plans.

(2) Space support operations consist of operations that launch, deploy, augment, maintain, sustain, replenish, deorbit, and recover space forces, including the C2 network configuration for space operations. Space support operations enable US space forces to

continue to provide vital space capabilities to military and civilian activities in defense of the homeland.

(3) Space force enhancement operations multiply the effectiveness of HD operations by enhancing operational awareness and providing needed warfighter support. There are five force enhancement functions: ISR; integrated tactical warning and attack assessment; environmental monitoring; SATCOM; and position, velocity, time, and navigation (primarily GPS). Force enhancement functions are also often provided by agencies such as the National Reconnaissance Office, NSA, National Geospatial-Intelligence Agency (NGA), National Aeronautics and Space Administration, National Oceanic and Atmospheric Administration, commercial organizations, and consortiums.

(4) Space force application consists of attacks against targets carried out by military weapons systems operating in or through space. The force application mission area includes ballistic missile defense and force projection.

c. **Integration of civilian space capabilities**. HD is a high-priority activity, requiring the marshalling of all available space capabilities. Key to maximizing US space capabilities is the successful integration of civilian space assets with military space capabilities. In many cases, especially in the area of SATCOM, environmental monitoring, and some space imagery, the contribution of civilian systems provide an integral part of the total US space capabilities. Use of civilian space capabilities is essential to the effectiveness of our ability to successfully accomplish the HD mission.

*For additional information, refer to JP 3-14*, Joint Doctrine for Space Operations.

## 3. Ballistic Missile Defense

Ballistic missile defense (BMD) capabilities are designed to detect, deter, defend against and defeat adversary ballistic missile threats. The goal is to build a layered, integrated capability to defeat inbound missiles in all phases of flight. The intent is to engage a target with multiple weapons systems through the depth and breadth of the ballistic trajectory of a missile. BMD involves passive defense, active defense, attack operations, and battle management. The BMD system consists of sensors (air, land, sea, and space), weapons (ground, air, and sea-based), C2, and manning and logistics systems, which are employed collectively. BMD of the homeland includes the synchronization and integration of capabilities to destroy or disrupt adversary missiles in flight or prior to launch. BMD fully synchronizes and integrates offensive and defensive actions and supporting systems to achieve unity of effort. BMD is a key element of HD, however, BMD activities do not include defense against cruise or tactical air-to-surface missiles.

a. **Command Roles and Responsibilities.** All combatant commands are tasked with deterring attacks against the United States, its territories, and possessions, and employing appropriate force should deterrence fail within their respective AORs. GCCs are responsible for planning and executing ballistic missile defense within their geographic AORs. CDRUSSTRATCOM is responsible for planning, integrating, coordinating and

advocating global missile defense operations and support. The following organizations are highlighted because of their specific BMD responsibilities to support HD. Further considerations can be found in the UCP and JP 3-01, *Countering Air and Missile Threats*.

(1) The CCDRs with geographic HD responsibilities deter ballistic missile attacks on the United States, its territories, possessions, and bases within the respective AORs, and other areas as directed. In coordination with CDRUSSTRATCOM and other GCCs, they synchronize support for the execution of operation plans to defend against ballistic missile attacks on the homeland, and should deterrence fail and/or as directed by the President or SecDef, they employ BMD forces in a synchronized operation to protect the United States against ballistic missile attacks.

(2) CDRUSSTRATCOM serves as a coordinating authority for global missile defense and is responsible for the following items:

(a) Planning, integrating, and coordinating global missile defense operations that cross AOR boundaries.

(b) Providing missile warning and space surveillance to NORAD to fulfill the US commitment to the NORAD Agreement.

(c) Providing warning of missile attack to all other CCDRs.

(d) Developing the concept of operations for global missile defense.

(e) Supporting other combatant commands in the development, assessment, coordination, and recommendation of ballistic missile defense.

(3) CDRUSSTRATCOM established the Joint Functional Component Command for Integrated Missile Defense (JFCC-IMD) to optimize planning, execution, force management and coordination with other combatant commands for USSTRATCOM's global missile defense mission. The JFCC-IMD accomplishes CDRUSSTRATCOM UCP responsibilities for global integrated missile defense planning, coordination, and integration and ensures day-to-day operational support responsibilities are coordinated. JFCC-IMD coordinates activities with associated geographic combatant commands, other USSTRATCOM joint functional component commands, and the efforts of the Missile Defense Agency.

b. **BMD Operations.** BMD employs the operational elements of missile defense to provide protection across the range of operations. Through the balanced employment of passive and active defense and dynamic attack operations, BMD ensures the desired end-state of attaining favorable ratios for ballistic missile defensive weapons. This is supported by shared situational awareness, integrated battle management C2, adaptive planning, and accurate and responsive battle damage assessment. For further discussions on missile defense refer to JP 3-01, *Countering Air and Missile Threats*.

c. **Related operations.** BMD has a direct relationship to several other HD (and CS) operations:

(1) **CM**. Employment of BMD assets for HD could result in situations requiring CM. CM operations may include responding to personal injury, property loss, or debris field cleanup resulting from BMD system engagements, or catastrophic failures during testing or fielding of BMD systems. For this reason the coordination of information between organizations planning or executing BMD operations with potential responders is critical.

(2) **DCI and FP**. BMD is also closely related to DCI and FP actions as there may be a requirement to establish a missile defense umbrella over a site that is designated as DCI, (e.g., a CONUS port of embarkation). CCDRs with geographic HD responsibilities must maintain a BMD priority defended asset list for the US homeland. It must be coordinated and in concert with DCI and FP programs.

(3) **Space operations**. Space operations are considered critical enabling activities for BMD. For example, space based surveillance and sensor capabilities provide ballistic missile early warning, assist in intelligence gathering, and facilitate tracking inbound missiles. For further space operation considerations reference JP 3-14, *Joint Doctrine for Space Operations*.

(4) **Combating Weapons of Mass Destruction**. JP 3-40, *Joint Doctrine for Combating Weapons of Mass Destruction*, contains doctrine on this joint mission that closely parallels BMD and air and missile defense in general. BMD planners should coordinate their attack operations and BMD efforts with these operations to optimize use of strike and attack assets, effectiveness of preemption measures and unity of effort.

Intentionally Blank

# CHAPTER VII
## OTHER SUPPORTING OPERATIONS AND ENABLING ACTIVITIES

*"I am telling you all, this is the defense mission of the next century -- homeland defense, fair and simple. It will take several different forms. Protection against terrorist attacks using chemical or biological weapons. Protection against attacks, cyber attacks from people using computers to bring down air traffic control systems or utility systems or whatever. And homeland defense against world errant nations using a ballistic missile or two. So homeland defense is the mission of the next century."*

**The Honorable John J. Hamre**
**Deputy Secretary of Defense (1998)**

## 1. General

Supporting operations and enabling activities should be considered in the planning and execution of all HD operations. They often overlap with other activities and specific tasks may be closely related. For example, when performing activities associated with DCI, planners must also consider AT and FP measures to protect Service members or specific facilities and equipment. Additionally, continued operation of information systems deemed vital to C2 is often reliant on IO to ensure computer networks are defended.

## 2. Information Environment

The "information environment" is the aggregate of individuals, organizations, or systems that collect, process, disseminate, or act on information; also included is the information itself. It is broad in scope and directly supports military operations in any operational environment. It offers a framework of three dimensions; physical, informational, and cognitive. The information environment supports the HD framework. The US conducts operations, including HD, in a complex, interconnected, and increasingly global operational environment. The information environment and activities conducted in each of the domains influence and shape each other. Certain US military operations in the information environment are known as IO.

a. **Information Operations.** IO is the integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. Properly implemented, IO conducted across the range of military operations will support defense of the homeland by affecting the attitudes and beliefs of potential adversaries and thus altering their behavior, specifically the planning and execution of aggressive and hostile acts against the United States. IO degrades their effectiveness and allows US defenses an opportunity to detect, interdict, and counter hostile acts. From a defensive perspective, IO protects DOD information systems, and thus enhances our situational awareness. IO also promotes accurate situational awareness for US decision makers charged with HD responsibilities. IO in general may involve complex legal and policy issues. Specifically, US citizens will not be targeted in IO. These issues do not prevent the application of IO for HD but temper it.

*Details on the employment of IO can be found in JP 3-13*, Information Operations.

b. **Intelligence.** Knowledge of the enemy is one of the fundamentals of joint warfare outlined in JP 1, *Doctrine for the Armed Forces of the United States*. Intelligence is the discipline that provides this knowledge and information to the commander about an adversary's capabilities, centers of gravity, and probable course of action. Additionally, intelligence assists the commander in visualizing the operational environment within which both the adversary and friendly forces operate. To be of operational use, intelligence must be timely, accurate, usable, complete, relevant, objective, available, and disseminated to those decision-makers and operators who need it for successful HD operations. Intelligence assessments help the commander determine the magnitude of the threat, which forces to deploy, the most efficient manner in which to deploy those forces, and probable enemy reactions.

(1) Fusion is the process of examining all sources of intelligence and information to derive a complete assessment of activity. This process, by its very nature, involves both automation and human cognition. Intelligence fusion is an on-going process that involves the delineation of roles and responsibilities; creation of requirements; collection; integration; analysis; and dissemination of critical information. This data can be derived from a multitude of sources, technologies, and human review (cognition).

(2) The operational integration of ISR platforms and sensors provides key information to decision-makers at all levels of command. ISR capabilities provide strategic, operational, and tactical commanders situational awareness to support the unity of effort for HD. Collecting data from multiple sources is essential to remove the bias of a source, improving the accuracy and completeness of the analysis. Additionally, it can defeat the enemy's denial and deception efforts. A synchronized collection effort across various sources and disciplines facilitates cross-cueing among collectors and a more efficient application of limited resources. CDRUSSTRATCOM established the joint functional component command for intelligence, surveillance, and reconnaissance (JFCC-ISR) to conduct planning to employ DOD ISR resources to meet national, departmental and combatant command requirements. Additionally, close and early coordination with JFCC-ISR provides access to and support from DOD and national ISR assets to support HD operations.

(3) Intelligence operations for HD present unique information sharing requirements for military intelligence and law enforcement entities. Each is governed by its own missions as well as applicable legal and policy constraints (see intelligence oversight, as outlined for DOD in Chapter I). The CCDRs with geographic HD responsibilities are the lead commands for planning and executing DOD HD intelligence operations. As such, they will coordinate with other DOD and national intelligence agencies and federal, state, tribal, and local entities. For HD, it is particularly important to ensure effective fusion of intelligence, counterintelligence, law enforcement, and other available threat information to develop a complete assessment of threats to the homeland and prevent strategic or tactical surprise.

(4) For USNORTHCOM, effective intelligence fusion is energized through interagency collaboration and spearheaded by the NORAD USNORTHCOM Joint Intelligence Operations Center - North. Under the direction of CDRNORAD and/or USNORTHCOM, the

Intelligence Directorate provides forums for information exchange, analysis, priorities, and strategy. The outcome of fusion provides decision makers and operators situational awareness and enables situational understanding. This enhances timely and effective decision making and supports successful operations and mission accomplishment.

(5) The joint intelligence process is continuous and includes the following steps: planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback. The dissemination and integration step is critical. Properly formatted intelligence products are disseminated to requesters, who integrate intelligence into the decision-making and planning process. The disseminated product can appear in multiple forms (e.g., voice reports, digital reports, formatted messages, estimates, or specialized products). Additionally, disseminated products can be categorized as indications and warning, general military intelligence, counterintelligence, and law enforcement information. Disseminating actionable intelligence to the user is fundamental to preparing for, preventing, responding to, and recovering from events.

*For more information on of intelligence fusion, see Joint Publication 2-0*, Joint Intelligence.

c. **Global Information Grid**

(1) As part of the overall information environment, the GIG represents the globally interconnected communications system of DOD. It includes the end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services.

(2) Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer (ASD(NII)/DOD CIO) is responsible for establishing and implementing a network operations (NETOPS) information exchange process and authoring agreements to support DOD operations and activities. The ASD(NII)/DOD CIO coordinates this process with the ASD (HD&ASA), who is responsible for coordinating all HD mission area matters with other executive departments and federal agencies.

(3) Consistent with laws and policy, Services, DOD agencies, and non-DOD agencies should provide capabilities to support combatant command requirements to ensure the interoperability, availability, shared situational awareness and understanding, and effectiveness of the HD information environment. This includes capabilities to deter, detect, respond, and mitigate virtual and physical attacks against defense information infrastructure that directly or indirectly supports HD missions.

(4) There are three primary aspects to providing an available and effective HD information environment. These are providing a reliable, robust HD communications

system; improving information sharing among HD mission partners; and assuring and defending our critical information infrastructure against threats and aggression.

d. **Communications System**

(1) The communications system enables centralized planning and the coordinated and mutually supporting employment of forces and assets. It includes command centers, operations centers, processing and distribution centers and associated systems, deployed systems, and data sources. Systems or information, and decisions generated by them, should be shared to the maximum extent possible to ensure synchronization of effort among mission partners. For example, the COP facilitates decentralized execution in rapidly changing operational environments and must be shared among appropriate agencies, to include law enforcement, to ensure consistent situational awareness.

(2) The AORs of the CCDRs with geographic HD responsibilities are rich with existing commercial communications systems that can be leveraged to the maximum extent possible. For example, commercial cellular capabilities represent a choice medium that can provide immediate capability. Traditional DOD communications systems will serve as the backbone in support of HD operations. Nontraditional systems that are scalable, interoperable, and complementary with those used by coalition and civilian partners, will be essential to augment traditional ISR and C2 nodes, especially in the early phases of military operations. These communications must be mobile, secure, and voice and data capable. Wireless voice, data, and video are critical to effective C2. Planning for the integration of spectrum resource allocation will enable DOD; federal, state, tribal, and local responders; IGOs and NGOs; and private sector responders to operate in the same bands, ensuring interoperability. Planning for the integration of internationally-donated telecommunications resources, including hardware and SATCOM bandwidth, should be conducted in the event the USG accepts such offers of international aid.

(3) Commercial infrastructure plays a critical role in enabling the communication systems that directly support HD operations. This infrastructure may be damaged to the point that military and supporting operations are adversely affected. DOD must identify capabilities that can help bridge the gap until local infrastructure is restored. These capabilities must be highly mobile, rapidly deployable, and commercially interoperable. In addition, DOD should seek innovative ways to leverage commercial technology (i.e., satellite and cellular capability). An example would be to foster a partnership with commercial industry to develop a concept similar to civil reserve air fleet for employment of commercial assets and manpower in response to HD. Another example would be to integrate interoperability with commercial communications and standards into DOD equipment during development and acquisition phases.

(4) The communications system directorate of a joint staff (J-6) is responsible for providing the communications system needed to support reliable and timely information flow in support of joint operations. The CCDR, through the communications system directorate, provides communications system guidance and priorities to supporting commands and components. The execution of theater guidance and priorities is through the

theater NETOPS control center (TNCC). To effectively do this, the TNCC must maintain situational awareness of critical communications systems in the AOR. The TNCC will coordinate and direct as required, communities of interest within the AOR to ensure accurate, timely, and detailed reporting on these systems. These communities of interest include subordinate commands, supporting commands, Services and agencies, as well as non-DOD organizations.

e. **Improving Information Sharing**

(1) Information sharing within DOD and the USG has undergone significant changes since 9/11/01. DOD must lead the way in transitioning from a "need to know" to a "need to share" culture. The need to share information is an operational necessity that avoids withholding information and minimizes the potential for operational gaps that characterized the pre-9/11/01 environment. The overall goal is to attain seamless access to the trusted information sharing environment for all response forces throughout the AOR. To accomplish this, DOD provides guidance and standards to ensure maximum flexibility and interoperability with mission partners.

(2) To improve information sharing, DOD along with its non-DOD partners, have initiated common solutions and data sets that ensure interoperability and allow them to communicate quickly and more accurately. A collaborative environment among HD mission partners is a critical aspect to facilitating information sharing and interoperability. It provides the ability to create and share data, information, and knowledge needed to plan, execute, and assess joint force operations, enabling a commander to make decisions faster than the adversary. The speed with which information is gained, processed (and if necessary, sanitized for required dissemination and/or sharing) and understood influences how well we engage during emerging events.

(3) The collaborative environment supports the multilevel partitioning of vital information to enable allied and coalition forces, as well as non-DOD mission partners, to participate in HD operations. Web technology, a standard set of collaborative tools and databases, and common protocols and access are solutions that enable a broader audience to more effectively share information.

(4) Proper organization of the battle staff support structure is another way to facilitate the synchronizing and sharing of information. NORAD and USNORTHCOM use an adaptive headquarters model for their staffs when organizing for specific operations and exercises. In the adaptive headquarters, the staff reorganizes from its traditional functional areas of personnel, intelligence, operations, logistics, plans, and communications, to working groups that address current operations, future operations, joint plans, joint support, and interagency coordination. The organization must also transcend culture, policy, and technical barriers to be effective.

(5) Within the NORAD and USNORTHCOM Headquarters Battle-Staff the information synchronization group (ISG) is an enabler of the collaborative environment and manages information flow and synchronization processes to improve the support of all

command elements. The ISG is responsible for synchronizing information and for facilitating information and intelligence sharing across the commands and the mission partners in support of HD operations.

(6) The primary ISG function is the fusion of all operationally relevant information across functional areas. The intent is to enable decision making by senior leadership resulting in timely actions for successful mission accomplishment. The ISG improves synchronization by employing information exchange brokers embedded within the various headquarters battle-staff elements, and subordinate commands. They are subject matter experts that facilitate information flow between headquarters elements, subordinate commands, and mission partners.

f. **Assuring and Defending Critical Information Infrastructure**

(1) The USG has a primary role for preventing and responding to threats in cyberspace and incidents and identifying and prosecuting the perpetrators. National policy for managing such threats and incidents is provided for by HSPD – 5, *Management of Domestic Incidents* and HSPD – 7, *Critical Infrastructure Identification, Prioritization, and Protection*, which establish national policy for mitigating vulnerabilities of our critical infrastructures to attack in cyberspace and for strengthening our capabilities to detect, prevent, defeat, and manage the consequences of cyberspace incidents. The National Response Plan (NRP) implements the national policy for incident response and the *National Infrastructure Protection Plan* implements the national policy for critical infrastructure protection.

(2) DHS's National Cyber Response Coordination Group (NCRCG) is the principal interagency mechanism for managing cyberspace incidents of national significance and other national cyberspace incidents and physical attacks that have significant cyberspace consequences. The NCRCG facilitates federal coordination of the various response activities conducted during a cyberspace incident pursuant to HSPDs 5 and 7, the NRP, and the inherent authorities of the agencies and departments that comprise the NCRCG. DOD has a statutory role in cyberspace security, cybercrime training, and protection of critical information infrastructure and key assets and is a member of the NCRGC.

(3) HD includes the protection of critical DOD networks and when directed, national networks against threats and aggression. This includes DOD critical information infrastructure. It is accomplished through *physical* and *virtual protection*.

(a) Physical protection of networks is the responsibility of all DOD components and non-DOD mission partners that own critical information infrastructure supporting HD missions. Combatant commands, Services, and agencies are supported in their physical protection efforts through the DCIP and the National Communications System (NCS). The NCS coordinates national security and/or EP communications for the USG as well as the communication emergency support function under the NRP. The National Coordinating Center (NCC) within the NCS serves as the Information Sharing and Analysis Center for the telecommunications industry. As such, the NCC and national coordinating

center functions as an important link within the telecommunications industry. This link can be exploited to assist in commercial circuit restoration. Additionally, the NCS provides access to all USG priority communications systems including the Government Emergency Telecommunications Service, the Wireless Priority System and the Telecommunications Service Priority system. The NCS, as the lead for the National Critical Infrastructure Protection Telecommunications Sector, can also assist in critical infrastructure analysis of the commercial telecommunications assets upon which DOD depends. The CCDRs with geographic HD responsibilities have established relationships with the NCS and coordinate on all commercial infrastructure restoral plans to ensure unity of effort.

(b) Virtual protection complements physical protection. For DOD, it is accomplished through NETOPS and DOD support to the NCRCG. NETOPS is the operational construct CDRUSSTRATCOM uses to operate and defend the GIG. NETOPS operators are responsible for performing the functions to sustain the operational readiness of the GIG. NETOPS provides integrated network visibility and end-to-end management of networks, global applications, and services across the GIG in support of DOD's full range of military operations. It assures the GIG will be available to support HD operations. The technical scope of NETOPS includes all GIG assets, the entire infrastructure, organization, personnel, procedures, and components that collect, process, store, transmit, display, disseminate, and act on information. There is no comparable program for non-DOD mission partners.

(c) A NETOPS event is a collective term for all NETOPS activities that have the potential to impact the operational readiness of the GIG. To effectively operate the GIG as a global enterprise while realizing the GCCs' requirement to direct GIG operations in their theaters, CDRUSSTRATCOM developed an event based C2 structure. C2 of GIG operations will be based on the situation at the time of an event. The two possible circumstances that determine the C2 of NETOPS are known as theater NETOPS events and global NETOPS events. Theater NETOPS events are under the control of the GCC and his Service components. Global NETOPS events occur less frequently, but when they do occur CDRUSSTRATCOM will direct the global response. USSTRATCOM, in conjunction with other CCDRs, establish tactics, techniques and procedures for executing the supported relationships within the NETOPS C2 structure.

(d) CDRUSSTRATCOM is the supported commander for global NETOPS events and issues orders and direction through Joint Task Force Global Network Operations (JTF-GNO) to the combatant commands, Services, and agencies and other members of the NETOPS community of interest. GCCs are responsible for leading the theater response to global NETOPS events within their theater in accordance with USSTRATCOM and JTF-GNO direction. JTF-GNO Service component commands will support the execution of global NETOPS. Functional CCDRs are the supported commanders where NETOPS activities affect or have the potential to affect execution of their assigned missions.

(e) The Intelligence Community Incident Response Center is the IC's single focal point for IC network incident reporting and management. Activities involving IC networks, specifically sensitive compartmented information networks, will be coordinated in

accordance with joint procedures approved by SecDef and the Director of National Intelligence. Due to the close interdependencies that DOD and IC components have on each other's networks, it is essential that reporting procedures be in place to ensure rapid coordination in network defense. Reporting on IC networks is accomplished through the JTF-GNO and shared with the TNCCs of the CCDRs with geographic HD responsibilities.

(f) The National Military Strategy for Cyberspace Operations (NMS-CO) offers a comprehensive military strategy for DOD to enhance US military strategic superiority in cyberspace. The NMS-CO addresses three main roles: defense of the nation, national incident response, and critical infrastructure protection. CCDRs with geographic HD responsibilities should ensure unified action at the theater level for cyberspace operations. This includes coordinating with coalition and interagency partners as outlined in strategy, policy, and agreements.

### 3. Defense Critical Infrastructure

DCI is the DOD and non-DOD networked assets essential to project, support, and sustain military forces and operations worldwide. Assets are people, physical entities, or information. Physical assets would include installations, facilities, ports, bridges, power stations, telecommunication lines, pipelines, etc. The increasing interconnectivity and interdependence among commercial and defense infrastructures demand that DOD take steps to understand and remedy or mitigate the vulnerabilities of, and threats to, the critical infrastructures on which it depends for mission accomplishment. The DCIP is a fully integrated program that provides a comprehensive process for understanding and protecting selected infrastructure assets that are critical to national security during peace, crisis, and war. It involves identifying, prioritizing, assessing, protecting, monitoring, and assuring the reliability and availability of mission-critical infrastructures essential to the execution of the NMS. The program also addresses the operational decision support necessary for CCDRs to achieve their mission objectives despite the degradation or absence of these infrastructures.

a. The DCIP complements other DOD programs and efforts, such as FP, AT, information assurance (IA), and COOP. Overall responsibility for protection of non-DOD critical infrastructure rests largely with DHS. One exception is the defense industrial base (DIB), which falls under DOD for protection. DCIP activities related to the DIB are consistent with and complement the authorities outlined in DOD Directive 5220.22, *National Industrial Security Program*. Information on DCIP plans, programs, and assets are safeguarded IAW pertinent DOD issuances on information security and OPSEC.

b. DOD serves as the sector-specific agency for the DIB with responsibilities to collaborate with all relevant entities, conduct or facilitate vulnerability assessments, and encourage risk management strategies. These responsibilities are outlined in HSPD-7, *Critical Infrastructure Identification, Prioritization and Protection,* and further expanded in the National Strategy for Physical Protection of Critical Infrastructure and Key Assets as well as the National Infrastructure Protection Plan. The ASD(HD&ASA) under the USD(P) acts as the principal staff assistant and civilian advisor to SecDef on DCIP activities and provides policy and strategy guidance. CJCS is the principal military advisor to SecDef on

DCIP activities and is responsible for the coordination, integration, prioritization, and guidance for DCIP operations. GCCs and Service Chiefs are responsible for operational assessments, planning, integration, and protection of DCI.

c. **CCDRs conducting HD missions are responsible for establishing a DCIP that conforms to DOD requirements and policy.** DOD components are also responsible for establishing similar programs. The components must identify and assess the critical assets and infrastructure dependencies that are necessary for the successful execution of present and projected military operations, their fulfillment of HD operations, and protection of US interests at home. Components also address these issues at the installation level.

d. Force projection capabilities consist of both DOD-owned and non-DOD-owned assets, facilities, and systems that enable DOD to project military power globally. Examples include strategic military bases, ports of embarkation/PODS, mobilization staging and storage areas, rail and trucking transportation centers, etc. Protection and defense of non-DOD facilities is normally coordinated with federal, state, tribal, and local LEAs; however, if directed by the President, DOD may be tasked to provide the forces and have the overall responsibility to defend these facilities.

*For more information concerning critical infrastructure protection (CIP) and the DCIP see DODD 3020.40, Defense Critical Infrastructure Program (DCIP).*

### 4. Combating Weapons of Mass Destruction

a. Combating WMD contributes to HD by protecting the United States, our allies, partners, and interests through an active, layered, defense in depth. In the hands of adversaries, these weapons could enable them to inflict massive harm on the United States, including our military forces at home and abroad. The National Strategy to Combat Weapons of Mass Destruction sets forth the three pillars: counterproliferation to combat WMD use, strengthened nonproliferation to combat WMD proliferation, and CM to respond to WMD use.

b. The military mission is to dissuade, deter, and defeat those who seek to harm the United States, its allies, and partners through WMD use or threat of use. This mission is in direct support of the three pillars. According to the National Military Strategy for Combating Weapons of Mass Destruction, the Armed Forces of the US may be called upon to carry out eight missions:

(1) Offensive operations.

(2) Elimination.

(3) Interdiction.

(4) Active defense.

(5) Passive defense.

(6) WMD CM.

(7) Security cooperation and partner activities.

(8) Threat reduction cooperation.

c. The global WMD threat has grown more complex and diverse including both state and non-state actors and the rapid advance of technologies to develop and deliver WMD. DOD plays an essential role in combating WMD through a full range of operational capabilities to protect the United States, our military forces, and partners and allies from the threat or actual use of WMD. For example, DOD is one of many participating USG departments/agencies which support the multinational PSI, the program supported by the United Nations Convention for the Suppression of Unlawful Acts at Sea and is designed specifically to counter the proliferation of WMD and precursors/material.

*For more information on Combating WMD see JP 3-40*, Joint Doctrine for Combating Weapons of Mass Destruction and *JP 3-41*, Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives Consequence Management, *and JP 3-11,* Joint Doctrine for Operations in Nuclear, Biological, and Chemical (NBC) Environments.

## 5. Sustainment

a. Personnel

(1) The core functional responsibilities of a joint force J-1, are accomplished during HD operations; with some exceptions such as, morale, welfare, and recreation; establishing a rest and recuperation program; coordinating military postal operations; monitoring joint personnel training and tracking activities; rotational policy planning; and identifying special pay and entitlements.

(2) A joint force J-1 may not be required to accomplish support and assistance to the office of primary responsibility for reserve component call-up, personnel recovery operations, noncombatant evacuation operations, and detainee operations during HD operations.

(3) **Personnel Support**. The authorities and responsibilities for personnel support to HD operations are largely the same as those for any other DOD mission set. Some notable exceptions, however, apply to HD operations within the land, airspace, and territorial waters of the US. More specifically, those exceptions apply to areas within the USNORTHCOM AOR.

(a) **Personnel Accountability**. Personnel accountability is a command responsibility. Personnel accountability, strength reporting, and manpower management are the focal points for a joint force J-1 during HD operations. HD operations in CONUS

pose specific challenges, one example being, units deploy from their home stations instead of a unique designated port of debarkation (POD). Service personnel elements supporting home station deployments must ensure that all processing and reporting requirements are met prior to unit deployment. In specific circumstance, such as operations in a WMD environment, the employing CJTF may establish a joint reception center to ensure arriving units are ready for employment, but this would be the exception.

(b) **Individual Augmentation**. USNORTHCOM forces are task organized when needed, causing a continuing requirement for individual augmentations. This particularly applies to AFNORTH, USARNORTH, and potentially MARFORNORTH in cases where they are required to form JTFs. These component commands must prepare joint manning documents listing the specific Service expertise required to meet their mission requirements. See CJCSI 1301, *Individual Augmentation Procedures*, for detailed guidance.

(c) **Personnel Accountability in Conjunction with Disasters**. Attacks on the United States can affect DOD personnel and their dependents. Service components account for and report the status of all DOD-affiliated military and civilian personnel, including contractor and all family members immediately following a disaster or attack. Additionally, Service components should be prepared to report the number of Service members, DOD civilians, DOD contractors and their dependents requiring evacuation from an affected area. See DODI 3001.02, *Personnel Accountability in Conjunction With Natural or Man-made Disasters*.

*For detailed guidance on Personnel Support, see JP 1-0,* Personnel Support to Joint Operations.

b. **Logistics**. The authorities and responsibilities for logistics operations in support of HD are largely the same as any other DOD mission set. Some notable exceptions, however, apply to HD operations within the land, airspace, and US territorial waters. More specifically, the exceptions apply to the USNORTHCOM AOR.

(1) JP 1, *Doctrine for the Armed Forces of the United States,* states that the "exercise of directive authority for logistics (DAFL) by a CCDR includes the authority to delegate authority for common support capability to subordinate commanders" and that "CCDRs exercise COCOM over assigned forces." Within the USNORTHCOM AOR the CDRUSNORTHCOM does not have assigned forces and therefore executes OPCON or TACON over attached forces without DAFL. Given the robust logistics capabilities within each Service component and DOD support agency/commercial contracting infrastructure in the USNORTHCOM AOR, DAFL is generally not necessary for CDRUSNORTHCOM to execute the HD mission. It may be necessary at times for CDRUSNORTHCOM to exercise DAFL in responding to an HD threat, or more specifically in reacting in the aftermath of an actual attack against the homeland. For such instances, the President or SecDef may extend this authority to attached forces when transferring those forces for a specific mission.

*For further information on logistic support refer to JP 4-0*, Logistic Support for Joint Operations.

(2) Implementation and execution of logistic functions remain the responsibility of the Services and the Service component commanders. Each Service is responsible for the logistic support of its own forces, except when logistic support is otherwise provided for by agreements with national agencies, allies or another Service.

(3) In the case where coalition operations are used for HD operations, coalition partners are ultimately responsible for providing logistic support for their own forces. However, the GCC should strive to negotiate, conclude, and integrate the use of acquisition and cross-servicing agreements and associated implementing arrangements and any other vehicle necessary to ensure needed logistics support.

(4) **Functions of Logistics.** Responsibilities for the functions of logistics as described in existing joint doctrine apply to HD operations with the following exceptions:

(a) **Supply**. USNORTHCOM will normally not establish supply buildup rates or determine theater stockage levels in the USNORTHCOM AOR. Based on mission requirements, Service components and DOD combat support agencies (CSAs) determine build up rates and stockage levels for supply.

(b) **Maintenance and Salvage**. Service components and CSAs will maintain administrative and coordination responsibilities for maintenance and salvage within the USNORTHCOM AOR.

(c) **Transportation.** HD airlift priorities are outlined in CJCSI 4120.02, *Assignment of Movement Priority*. The national importance of these mission areas is reflected in the elevated movement priorities that can be applied for these missions by the President or SecDef. For operations that demand expedited movement, CDRUSTRANSCOM will maintain on-call readiness levels necessary to meet CDRUSNORTHCOM mission requirements. The NORAD-USNORTHCOM Deployment Distribution Operations Center (NDDOC) is embedded within the Joint Support Center and is composed of personnel from NORAD and USNORTHCOM and national partners as required (i.e., US Transportation Command [USTRANSCOM], Defense Logistics Agency [DLA], the Services, and other organizations). It is established as directed by CDRUSNORTHCOM to support HD (and CS) operations and operates under the direction of the NORAD-USNORTHCOM J-4. The NDDOC implements command movement priorities, anticipates and resolves transportation shortfalls, prioritizes transportation assets, synchronizes deployment force flow and distribution, and provides in-transit visibility.

(d) **Mortuary Affairs.** USNORTHCOM is responsible for controlling and coordinating mortuary affairs operations within its AOR. The local or state medical examiner or coroner will maintain jurisdiction over both military and civilian fatalities, unless the Armed Forces Medical Examiner requests and receives jurisdiction. However,

DOD should also be prepared to assist with fatality management operations and emergency family assistance to DOD families.

*See JP 4-06,* Mortuary Affairs in Joint Operations, *for details.*

(e) **Combat Service Support (CSS).** CSS enhances combat capability and improves productivity by providing life-sustaining and essential services and critical supply, maintenance, and transportation services to enable the operating force to conduct HD missions, supporting force reception and beddown across the range of military operations. The primary focus of the CSS effort is to sustain and assist DOD forces employed in HD.

(5) **Joint Reception, Staging, Onward Movement, and Integration (JRSOI)**. JRSOI is the essential process that assembles deploying forces, consisting of personnel, and equipment, and materiel arriving in theater, into forces capable of meeting the CCDR's operational requirements. In the USNORTHCOM AOR, portions of JRSOI identified below, are not appropriately regarded as discrete steps necessary for HD operations:

**Base Support Installation (BSI)**

**A BSI, when approved by the Secretary of Defense, serves as the main logistical hub for military support operations. Generally, most forces will deploy through, and the majority of sustainment will be positioned at the BSI. As a minimum, a BSI will normally have the following characteristics: an airfield and communications infrastructure sufficient to meet the surge of forces into an operational area, dry open areas for staging of supplies and equipment, a good road network, health and other life support services to include billeting, food service and force protection and be close to the focus of military operations/support to remain responsive and flexible to the needs of the joint force.**

(a) JRSOI for a large force can/will most likely require resources beyond that of the designated base support installation (BSI). The supported CCDR must request sufficient JRSOI support to ensure that the designated BSI can perform JRSOI.

(b) Reception operations include all those functions required to receive and clear unit personnel, equipment, and materiel through the POD. For HD operations within the USNORTHCOM AOR, the personnel, equipment, and materiel may originate from within the JOA. In that case, personnel, equipment, and material are already accounted for at the home base, making the home base essentially the POD. Component support plans will address processes for in place personnel reporting to the CJTF.

(c) Staging assembles, temporarily holds and organizes arriving personnel, equipment, and material in preparation for onward movement. Similarly to reception, the personnel, equipment, and material to be employed for HD operations within the USNORTHCOM AOR may stage within the confines of their home installation.

(d) Onward movement is the process of moving units and accompanying material from reception facilities, marshalling areas, and staging areas to tactical assembly

areas (TAAs) and/or operational areas or other theater destinations. Because units and forces likely to be employed in HD operations within the USNORTHCOM AOR are likely to be geographically close to the JOAs, the TAA can be located at the unit's or force's home base. Onward movement, in many instances, can be accomplished concurrently with and collocated with reception and staging activities – at the home base. When a unit or force is not geographically close to an operational area and a TAA other than the home base is desired, then traditional, discrete onward movement activities would be required. Oftentimes, a TAA would be located at a designated BSI that would provide logistic support and be located near the operational area.

(e) Integration is the synchronized hand off of units into an operational commander's force prior to mission execution. HD operations within the USNORTHCOM AOR often require complex C2 structures, thus special attention to integration is required. Refer to Appendix A, "Transitioning Between Homeland Defense and Civil Support."

c. **Engineering.** Military Engineering support may be required simultaneously for HD and CS operations. The primary focus of engineering effort is to sustain and assist DOD forces employed in HD. The secondary effort will be CS, when requested and approved IAW DOD guidance and applicable plans. The scope of engineering support for HD focuses on AT and/or FP construction, force bed-down, and emergency stabilization and repair of damaged critical infrastructure.

(1) **Planning Considerations**. The duration and scope of DOD engineer involvement will be directly related to the severity and magnitude of the threat, situation, or actual event. Engineer planners working either contingency or crisis action planning should develop plans with forces capable of initial tasks and priority of effort. Engineer efforts in HD may evolve into CS engineer actions. Initial planning considerations should address but are not limited to the following:

(a) Necessary AT and/or FP temporary construction.

(b) Force bed-down construction.

(c) Expedient hardening measures for enhanced facility, area, and/or asset survivability.

(d) Emergency stabilization and repair of damaged critical infrastructure.

(e) Emergency clearance of debris from airfields, roads, bridges, ports, wharfs, tunnels and waterways necessary to allow access to critical areas.

(f) Humanitarian needs of the dislocated populace, such as the construction of temporary shelters and support facilities.

(g) Repairs/work-arounds to other critical public utilities, services, and facilities that will help restore the ability of the local authority to manage its own recovery efforts.

(h) Demolition of damaged structures/facilities.

(i) Other support to federal agencies and emergency support functions outlined in the NRP.

(j) Use of geospatial intelligence products.

(2) **Engineer Assets and Capabilities.** DOD engineer capabilities coupled with the commercial sector/contract capabilities provide extensive engineering depth and breadth.

(a) A total force perspective for achieving engineering objectives is necessary. Engineer support may be garnered from local, state and federal resources via a multitude of avenues or agreements. In all respects, maximum consideration will be given to the use of locally available facilities, support structures, and contract services.

*For more information on DOD engineering organizational structures and assets, see JP 3-34*, Joint Engineer Operations.

(b) State active duty NG engineer forces may be operational within the AO or incident area along with Title 10 USC engineer forces. All engineer forces should seek to coordinate efforts to maximize capabilities and results.

(c) Deployable assets for force beddown are primarily in the Army Force Provider, Navy Advanced Base Functional Components and Air Force Basic Expeditionary Airfield Resources equipment sets. Leasing, modification to existing DOD infrastructure, and expedient construction should also be considered as a primary source for beddown support. Expedient construction includes several types of rapid construction techniques such as prefabricated buildings, inflatable buildings, etc. Flexibility in forces and methodology of execution is essential to successful HD engineer operations.

(d) Contractor support has become an essential part of DOD engineering capabilities. HD planning and execution for engineer missions should maximize the use of contract resources where and when the use of contractors is economical and does not negatively impact HD mission accomplishment. Sufficient local contractors are expected to be available to support most heavy equipment and engineer and construction requirements. Coordination with DOD agencies with large-scale contract capability such as the US Army Corps of Engineers (USACE), Naval Facilities Engineering Command (NAVFAC), Air Force Civil Engineer Support Agency and Air Force Center for Environmental Excellence should be conducted to ensure efficient resource utilization and gain economies of scale when possible.

(e) HD operations may include engineering forces from countries with international agreements/treaties such as the Canada-US Combined Defense Plan and Civil Assistance Plan. These forces may be made available to support operations, particularly if an event occurs in close proximity to adjacent country boundaries and should be considered during mission planning.

(3) **Engineers' Constraints.** Disruption of the commercial sector transportation, communication, and supply systems as well as limited DOD airlift support, competing DOD HD forces and the exigency of engineer mission requirements may have an adverse effect on HD engineer missions during crisis operations.

(a) Several broad authorities have been established under Title 10 USC that may enable the responding force to carry out emergency and contingency construction, to include procuring materials for construction by military forces and funding of contracts in support of contingency operations. When required, protective construction shall be in accordance with the unified facilities criteria (UFC), *DOD Minimum Standards for Buildings, UFC 4-010-01* and supporting Service standards.

(b) A catastrophic event may limit or place significant competing demands for Class IV materials. It is crucial that engineers articulate requirements for materials as expeditiously as possible. Expedient construction methods may be required when the HD action/situation limits time, material, manpower, or equipment.

(c) Acquisition of real property is not anticipated. However, short-term leasing may be necessary depending on location and duration forces are deployed. To the maximum extent possible, deployed forces will rely on the host of the critical infrastructure facility, the BSIs, or existing DOD facilities for real estate needs. Occupation of private land or facilities is not authorized without specific legal authority. Necessary rental/leasing support may be obtained from the General Services Administration, USACE, NAVFAC, or other government agency with an appropriately warranted contracting officer.

*For additional information on engineer organizations and assets of DOD military Services, see JP 3-34*, Joint Engineer Operations.

(4) **Environmental Considerations**

(a) **Environmental Responsibilities**. Military commanders are responsible for employing environmentally responsible practices that minimize adverse impacts to human health and the environment. During all operations, strategies will be developed to reduce or eliminate negative impacts on the environment. Similarly, strategies will be developed to minimize negative impacts to mission accomplishment caused by environmental degradation.

(b) **Planning Considerations**. Environmental considerations are an integral part of HD planning. Contingency planning for HD must include environmental considerations in planning and executing operations. Operational alternatives that minimize

damage to the natural environment or cultural/historic resources must be considered. HD actions undertaken during crisis are considered emergency actions, whereby national security and protection of life or property are at risk. HD response in crisis circumstances may make it necessary to take immediate actions without preparing the normal environmental planning documents. Compliance with applicable federal, State, tribal and local laws during crisis circumstances is still a DOD goal to the maximum extent possible.

(c) **Environmental Actions in the operational area.** DOD forces should make every effort to document environmental conditions upon arrival in the operational area as well as documenting conditions upon departure. Documenting actions as soon as possible during and after operations will facilitate resolution and closure of environmental issues. An active environmental review of HD operations should be accomplished to identify possible environmental issues before a negative impact occurs. Close liaison/communication with the applicable DOD regional environmental coordinator will also aid in ultimate resolution of environmental issues with, federal, state, tribal, and local agencies.

(d) **Remediation and Transfer to Civil Authorities.** Environmental impacts will be addressed as soon as possible once the operations have stabilized. Environmental HD incidents may evolve from actions or operations where DOD is not the federal agency with lead authority. Emergency exemptions may be needed for disposal of contaminated and hazardous material. DOD's goal is to initiate actions as soon as possible to curtail further environmental damage and to resolve environmental impacts. DOD forces should direct efforts to properly identify, contain, document, and transfer environmental issues to civil authorities as soon as possible.

d. **Religious Support**. Religious support (RS) is defined as the full spectrum of professional duties performed by chaplains in their dual role as religious leaders and military staff officers. Chaplains support military forces conducting HD as part of a religious support team (RST). The RST normally consists of at least one chaplain and an enlisted assistant of the same service.

(1) **Principles for Religious Support during HD**

(a) **Command Responsibility**. Military commanders are responsible for providing all authorized DOD personnel the opportunity to exercise their religious beliefs. RS for joint forces conducting HD is provided by service components and JTFs. RS during multinational events will be governed by appropriate agreements and plans with consideration for cultural differences and the commander's guidance.

(b) **Free Exercise and Accommodation**. Free exercise of religion is the constitutional right of every American. The primary role for military chaplains is to provide for the free exercise of religion for DOD personnel, to include service members, their families and authorized civilians. See DOD Directive 1300.17, *Accommodation of Religious Practices Within the Military Services*.

(c) **Joint Area Religious Support**. Joint area RS is religious support provided to all DOD personnel, regardless of service component or status, who are not part of the RST unit of assignment. As a primary mission, the RST will support the command to which assigned. When directed, the RST may also be responsible to provide joint area religious support to units without assigned chaplains, and to personnel from shortage or minority faith groups. As an example, a JTF may instruct chaplains in assigned units to provide RS to personnel from other services or components. In addition, an AC RST, when directed, may provide RS to NG personnel serving in state active duty or Title 32 USC (state controlled, federally funded) status during emergencies or exigent circumstances. Likewise, under these same circumstances, NG chaplains may provide joint area RS to AC personnel in Title 10 USC status if they are directed by the applicable joint force headquarters – state commander, and if the RS is conducted in accordance with state law. As an auxiliary of the Air Force, Civil Air Patrol chaplains are available to perform chaplain services on military installations or in performance of duties requested (see Air Force Instruction 10-2701, *Organization and Function of the Civil Air Patrol*).

(d) **Guidance for Military Chaplains during HD**. The RST will follow command direction, joint doctrine, supervisory chaplain guidance and legal counsel regarding permissible chaplain activities in the homeland.

e. **Force Health Protection and Health Service Support (HSS)**

(1) FHP, the protection component of HSS, provides the framework for optimizing health readiness and protecting Service members from all health threats. FHP complements FP. FHP includes all measures taken by the JFC and the Military Health System to promote, improve, conserve, or restore the mental and physical well-being of Service members across the range of military activities and operations. The JFC is responsible for FHP and must ensure that adequate HSS capabilities are appropriately planned for and in place to provide prevention and protection against health threats, and medical and rehabilitative care to maintain a healthy and fit force. The goal of HSS for HD is to minimize both disease and nonbattle injury (DNBI) and battlefield injuries (BIs) to support mission accomplishment.

(2) HSS provides services that promote, improve, conserve, or restore the mental or physical well-being of our forces. Specialized HSS capabilities characterize the potential occupational and environmental health (OEH) threats and provide commanders at all levels, risk mitigating recommendations to facilitate deployment preparation, prevent casualties, injury, and illness that occur in the field; and sustain operations. HSS is normally organized and determined by factors that include, and are not limited to: the joint force's mission, intelligence, population-at-risk, duration and scope of the operation, and the threat (to include OEH threats).

(a) The provision of HSS for HD missions varies significantly from conventional combat operations. HSS concepts for response to HD missions should focus

on the augmentation and expansion of medical capabilities found on installations, as an alternative to the projection of forces.

(b) Placing medical response capabilities at the installation level minimizes the burden on limited transportation assets, reduces the deployed footprint and advocates steady-state relationships between HSS organizations and community counterparts. The USNORTHCOM joint regional medical planners and USPACOM command surgeons are vital to coordinating this effort.

(3) **Health Threat and Medical Intelligence**. The health threat is a composite of ongoing or potential adversary actions; occupational and environmental threats; the employment of WMD; and endemic diseases that can reduce the effectiveness of the force through wounds, injuries, illness, and psychological stressors. Medical intelligence merges the capabilities of the medical and intelligence communities to gain a better understanding of potential threats, and identify mitigation and response options to minimize potential impacts.

(a) Through proactive analysis and increased situational awareness, medical intelligence is an essential component in understanding the threat environment and formulating policy and response options. Medical intelligence data is critical for the JFC to attain situational understanding of health threats; develop FHP and HSS policies and strategies that mitigate natural and intentional incidents; attain information superiority for the deterrence, prevention, mitigation and destruction of CBRNE threats and aggression; and redefine the battlespace from a medical perspective by employing strategic and preventative HSS response planning.

(b) In general, the US states and territories in the AORs of the CCDRs with geographic HD responsibilities are at low risk for endemic diseases during normal state of affairs. However, pandemic disease outbreaks have the potential to rapidly place the US military and wider population at risk. Nevertheless, man-made hazards (deliberate or accidental) may present the greatest potential health risk to forces conducting HD operations. Additionally, the physical areas of the homeland are heavily industrialized and have the potential for the accidental or deliberate release of a large variety of toxic industrial chemicals/materials at production sites and during transportation.

(4) **Health Surveillance**. Health surveillance is critical to FHP and includes the following activities: identifying the population at risk; identifying and assessing potential OEH hazards, documenting OEH and CBRNE risks and exposures; using specific risk management countermeasures; monitoring real-time health outcomes (medical surveillance); and reporting DNBI and BI rates and other measures in a timely manner. OEH surveillance is a key component of health surveillance and a key contributor toward DNBI prevention. Environmental and occupational monitoring for chemical, biological, and physical hazards such as indigenous communicable diseases, vectors, toxic industrial materials, field sanitation problems, and unsafe food and water is a continuous process over the entire deployment life cycle. During the pre-deployment phase, intelligence preparation activities must consider the available strategic and operational medical intelligence

pertaining to the operational environment to identify and protect against expected threats that may be encountered. The employment of appropriate HSS capabilities to provide comprehensive occupational, environmental, and operational exposure surveillance for forces deploying in support of HD operations is essential to the HD mission. Exposure surveillance must serve the real-time operational risk management decisions of the supported JFC. Additionally, exposure surveillance should be employed to conduct a retrospective analysis to improve force health protection for future operations and support follow-on medical care to previously deployed forces.

(5) **Medical and Health Related Tasks.** To support mission accomplishment and ensure effective and synchronized FHP and HSS for HD, CCDRs, Service, and component commands, should give consideration to the tasks provided below.

(a) CCDRs with geographic HD responsibilities should:

1. Develop FHP implementing guidance and directives in coordination with the Office of the Secretary of Defense (OSD), the Joint Staff, component commanders, the Services, NGB, DOD agencies and other unified commands.

2. Plan, coordinate and execute FHP and HSS tasks with component commands, other DOD components, state health authorities, interagency and multinational partners at the federal, state, tribal, and local levels.

3. Integrate medical intelligence, environmental surveillance, and syndromic surveillance efforts in collaboration with DOD components and other federal agencies via early warning systems to identify potential health threats.

4. Identify, prioritize, and coordinate risk mitigation for DOD health sector critical infrastructure in coordination with the OSD, the Joint Staff, component commanders, the Services, NGB, DOD agencies and the private sector.

5. Standardize and provide oversight for the health service aspects of vulnerability assessments.

6. Develop, establish and maintain patient movement operation plans, in coordination with CDRUSTRANSCOM.

7. Designate medical facilities at installations within the AOR to serve as regional medical response activities to coordinate and synchronize joint HSS in an operational area or medical support area to support an appointed CJTF.

8. Ensure awareness of bed capacity across the AOR. Obtain surge capacity data from national disaster medical system partners on a recurring basis.

(b) Joint force providers (US Joint Forces Command [USJFCOM], USTRANSCOM, USSTRATCOM, USSOCOM, Services and geographic combatant commands with assigned forces) should:

1. Plan, coordinate and execute FHP program IAW USNORTHCOM, USPACOM, USSOUTHCOM, DOD, CJCS, and Service directives and guidance.

2. Joint force providers should also ensure all deploying forces and capabilities have met pre-deployment FHP requirements specified in the EXORD.

(c) Functional component commands (JFMCC, JFLCC, and JFACC) should:

1. Plan and coordinate FHP implementation with other JFCs, DOD components, state health authorities, interagency and coalition partners at the local, state and regional levels. Component commands should also implement FHP directives in coordination with DOD components.

2. Be prepared to assume FHP and HSS responsibilities for forces or capabilities made available to the functional component. Responsibilities include ensuring adequate HSS capabilities (to include preventive medicine assets) are requested and deployed to ensure comprehensive exposure assessments and health risk management as defined in FHP guidance documents.

(d) NGB should:

1. Plan, coordinate and execute an FHP program IAW directives and guidance from the CCDR's with geographic HD responsibilities, DOD, CJCS, and Services.

2. Ensure all deploying forces have met pre-deployment FHP requirements specified in the EXORD. Additionally, ensure deploying forces meet post-deployment FHP requirements.

(e) **DOD agencies should:** Plan, coordinate and execute an FHP program IAW directives and guidance from the CCDR's with geographic HD responsibilities, DOD, CJCS, and Services.

(f) USTRANSCOM should:

1. Establish patient movement guidance in coordination with the CCDRs with geographic HD responsibilities in response to an attack on the homeland in their respective AORs. Joint patient movement in support of HD within the USPACOM AOR is in accordance with the USPACOM HD plan, and is the responsibility of the USPACOM theater patient movement requirements center (TPMRC). Per the USNORTHCOM HD plan, the global patient movement requirement center under USTRANSCOM serves as the TPMRC responsible for joint patient movement in the USNORTHCOM AOR in support of HD.

2. Provide patient movement planning and requirements identification for the USNORTHCOM AOR and validate CONUS patient movement missions.

3. Plan to establish or augment joint patient movement requirement centers (to include patient movement requirement centers for the national disaster medical system) to support HD contingency operations.

(g) **Joint Blood Program Office should:** Manage and coordinate all aspects of DOD blood product support and DOD blood distribution assets (in the AORs containing the homeland) in coordination with the Armed Services Blood Program Office (ASBPO).

# APPENDIX A
# TRANSITIONING BETWEEN HOMELAND DEFENSE AND CIVIL SUPPORT

## 1. General

a. Relationships between Homeland Defense, Civil Support, and Homeland Security.

(1) The homeland is confronted by a spectrum of threats and hazards. Some of these threats are ambiguous; essentially they are neither traditional military threats requiring only a DOD response capability, nor are they purely law enforcement threats requiring a nonmilitary response from DHS, DOJ, or another civilian agency. For example, a transnational threat can present a challenge in assigning lead responsibility to a particular agency. The characterization of a particular threat may, ultimately, rest with the President, but USG efforts are on-going to develop specific protocols and response options that address the coordination, integration and responsibilities of the federal agencies in responding to the full spectrum of threats and hazards. These new strategies, processes, and procedures are emerging out of documents such as the NSMS and US Aviation Security Policy, and their respective supporting plans (e.g., MOTR and AOTR Plans). These processes aid both the warfighter and civil authorities in identifying which agency or agencies are best suited to achieve the USG's desired outcome given the unique circumstances of the event.

(2) HS, as defined in the NSHS, is a concerted national effort to prevent terrorist acts within the United States, reduce America's vulnerabilities to terrorism, and minimize the damage and recover from attacks that do occur. However, the NSHS addresses HS beyond the definition, and includes law enforcement, CBRNE CM, and disaster preparedness and relief missions. Either DHS or DOJ will usually be the federal agency with lead responsibility, and supported by DOD, when requested. The NSHS addresses a very specific and uniquely challenging threat—terrorism against the United States—and provides a comprehensive framework for organizing the efforts of federal, state, tribal, local, and private organizations whose primary functions are often unrelated to national security. The NSHS complements the National Security Strategy (NSS) of the United States and provides a framework for creating and seizing opportunities that strengthen our security and prosperity. The Secretary of Homeland Security is responsible for ensuring the preparedness of the Nation to prevent, respond to, and recover from threatened and actual domestic terrorist attacks, non-terrorist security threats (e.g., drug and migrant smuggling), major disasters, and other emergencies.

(3) DOD protects the homeland through two distinct but interrelated missions – HD and CS. While these missions are distinct, some department roles and responsibilities overlap, and operations require extensive coordination between lead and supporting agencies. Figure A-1 illustrates a notional relationship between HD, CS and HS lead and supporting relationships with examples of the types of operations that can take place for each mission. The HD, CS, and HS missions are separate, but have areas where roles and responsibilities may overlap and/or lead and supporting roles may transition between organizations. DOD serves as the federal agency with lead responsibility for HD, which may be executed by DOD alone (e.g., BMD) or include support provided to DOD by other agencies such as DHS or DOT (e.g., FAA support to DOD/NORAD). CS is the overarching term for DOD's support to civilian authorities. DOD's role in the CS mission consists of

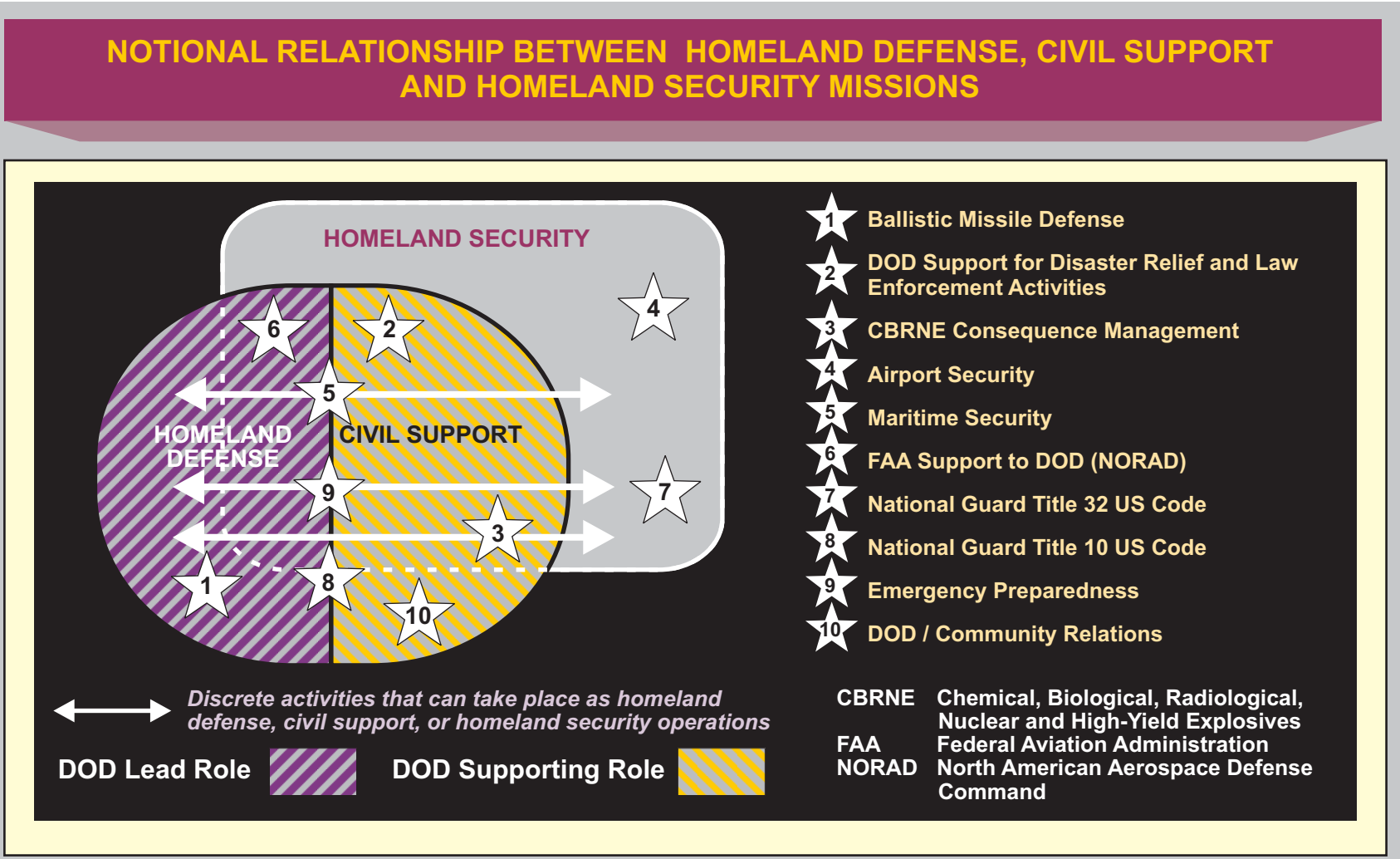



**Figure A-1. Notional Relationship Between Homeland Defense, Civil Support, and Homeland Security Missions**

support to US civil authorities (DHS or other agency) for domestic emergencies and for designated law enforcement and other activities. HD and CS operations may occur in parallel and require extensive integration and synchronization. In addition, operations may also transition from HD to CS to HS or vice versa (e.g., maritime security) with the lead depending on the situation and USG's desired outcome **(annotated by the arrows)**. **While the lead may transition, a single agency has the lead at any given time for a particular activity.** However, in the areas of overlapping responsibility, the designation of federal agency with lead responsibility may not be predetermined. In time-critical situations, on-scene leaders are empowered to conduct appropriate operations in response to a particular threat. The MOTR protocols provide guidance for maritime security, that can transition between HD, CS, or HS (see Chapter V, Maritime Operations). The NG and the reserves also play a vital role in the defense of the homeland. In the HD, CS and HS construct, the NG Title 10 USC authorities are depicted with HD and CS under DOD command and control (i.e., the NG can conduct HD and CS under Title 10 USC). Title 32 USC authorities are depicted as HS under the state or territory's command and control. Details on the employment of the NG for these missions are provided later in this appendix. EP is considered a part of DOD's overall preparedness activities. It spans HD, CS and HS and includes DOD's lead, support, and enable functions. Mobile command centers and DOD aviation support to the US Secret Service are just two examples of how DOD prepares for and supports EP operations.

## 2. Command and Control Options for Transition

In DOD, integration includes the synchronized transfer of units into an operational commander's force prior to mission execution. HD operations require special attention to integration, since the C2 possibilities are extensive. Traditional considerations for integration are adequate when DOD is the lead and is defending against traditional external threats/aggression. However, when DOD is simultaneously performing HD operations and supporting DHS or other federal agencies, the C2 becomes more complex. DOD uses military command structures, while the USCG and other federal, state, and local agencies utilize the Incident Command System, as adopted by the National Incident Management System. While they both provide the requisite C2, additional considerations regarding interagency coordination are required when transitioning to CS operations.

a. CCDRs cannot predict when an HD operation will transition to CS or vice versa. Additionally, CCDRs may be called on to execute HD and CS simultaneously. C2 in support of HD and CS operations must have a straightforward C2 template that will permit the CCDR to respond as the supported commander, supporting commander, or both. Recent changes in law and DOD policy have increased the CCDR's C2 options. Options include using a standing JTF headquarters, augmenting a core Service component headquarters, or forming an ad hoc organization from various contributors. When organizing C2 involving state NG forces, the CCDR may also seek appointment of a "dual status" commander. Regardless of the organizational structure, there are fundamental rules for forming and operating a JTF.

*For details on forming a JTF, refer to JP 3-33*, Joint Task Force Headquarters.

b. **NG Dual Status Commander**. A unique C2 relationship may be established when Title 10 USC and NG (Title 32 USC) forces operate together. Title 32 USC Section 325 allows a single commander to still fulfill NG requirements while serving on active duty if in command of a National Guard unit—if the President authorizes such service in both duty statuses; and the governor of the NG state or territory or the Commanding General of the District of Columbia NG, as the case may be, consents to such service in both duty statuses. A NG dual status commander retains his state NG commission when ordered to active duty under Title 10 USC. However, if a NG officer is activated to command an AC unit only, then NG requirements cannot be fulfilled by this section of Title 32 USC. As such, the "dual status" commander is able to command NG and federal Title 10 forces via separate state and federal chains of command.

c. **Title 10 Dual Status Commander**. Title 32 USC, Section 315 authorizes a Title 10 USC officer to obtain a state NG commission as detailed by the Secretary of the Army. By doing so, a Title 10 USC commander may command both state NG and Title 10 USC forces via separate state and federal chains of command. An officer so detailed may accept a commission in the NG without prejudicing his rank and without vacating his regular appointment. A Title 10 USC dual status command also requires the consent of both the President and the state governor involved.

d. A memorandum of agreement (MOA) must be signed by the governor and the President or their respective designees before a dual status command can be established. The MOA should be prepared by staff judge advocates (SJAs) from both chains of command to ensure the concerns of both are addressed. The dual status commander will receive orders from a federal chain of command and a state chain of command. As such, the dual status commander is an intermediate link in two distinct, separate chains of command flowing from different sovereigns. While the dual status commander may receive orders from two chains of command, it must be recognized that the dual status commander has a duty to exercise all authority in a completely mutually exclusive manner, i.e., either in a federal or state capacity, but never in both capacities at the same time. Additionally, the assigned or attached forces are not dual status. Thus, the commander should take care to ensure the missions of the forces are kept separate. This is best accomplished by maintaining separate staffs for the NG and Title 10 USC forces; especially separate J-2s, J-3s, and legal advisors, so that the separate chains of command remain distinct.

e. The intent of dual status command is coordination of operations to achieve unity of effort. The NG may be the first military organization engaged at the state level at the incident area. The NGB Joint Operations Center (JOC) in coordination with joint force headquarters – state JOCs provide situational awareness and status information to the combatant command and other federal stakeholders as the "first line of situational awareness." Likewise, due to the NG's proximity and speed of response, the CCDRs must leverage NG resources and capabilities, including existing C2 structures, into HD operations. Ultimately, the C2 structure should have the flexibility to rapidly transition from one mission set to another to ensure the efficient provision of assistance required from DOD as a supporting agency, per the NRP and the successful conduct of HD operations.

## 3. Planning Considerations for Transition

a. **Employment of RC Forces**. All RC forces are structured and operated to support assigned requirements. These requirements are based on mission assignments derived from the incident that the reserve force capabilities meet. Army Reserve forces supporting these operations are accessed either through Presidential reserve call-up (PRC) under Title 10 USC Section 12304 or by direct activation under another status. Mobilization under PRC or activation under annual training, active duty training, or active duty special work are accomplished from the unit's home station as a direct employing unit for US based operations. RC resources (personnel, equipment, and skills) should be appropriately leveraged and effectively integrated into DOD's HD and CS plans and operations. The USAR, USNR, USAFR, USMCR, and USCGR operate under the same C2 relationships at all times, whereas the ARNG and ANG also have a Constitutionally mandated responsibility to provide military support for state/territory requirements which are performed under the C2 authority of their respective governors unless they are formally mobilized to Title 10 USC status. Although the NG can also be employed in Title 10 USC status in support of HD missions, Title 32 USC Section 902 authorizes SecDef to provide funds to state governors for NG forces to perform specified HD activities without first activating these forces under Title 10 USC status. Title 32 USC Section 502(f) also provides authority for SecDef and the President to use the NG in a Title 32 USC status for other duty missions and operations, which may include domestic operations when appropriate. When placed on active duty, all RC forces conduct HD operations under Title 10 USC guidelines exactly as AC forces, and are subject to the provisions of the Uniform Code of Military Justice.

(1) **NG Forces.** The unique ability of the NG to function in either a federal (Title 10 USC) status or state (Title 32 USC) status must be considered for effective planning and should be leveraged to optimize DOD's preparedness to execute both HD and CS missions. The following are key planning factors that apply to optimally leverage NG forces for HD and CS:

(a) The homeland is a unique operational environment due to the need to achieve unity of effort within a constitutionally mandated relationship between federal and state governments as it impacts on military operations. HD operations are often described as those in which DOD is the federal agency with lead responsibility, whereas CS operations are those in which DOD supports another federal agency. Whereas this distinction is fairly unambiguous in missions such as air defense, which is often accomplished by the ANG assets transitioning between federal and state status through the use of "standing orders," it is not so straightforward when applied to missions such as prevention of or response to, critical infrastructure, CBRNE, or attacks in cyberspace, where clear procedural employment in a federal status has not been established. Executing these missions will require consideration of the laws, emergency management capabilities and processes, and existing interstate/territory arrangements established within each of the individual states and territories. The NG, by virtue of its unique ability to function in both a state and federal status and community-based presence is a de facto forward military presence throughout the 54 states and territories which has capabilities that can be readily leveraged for HD mission

support as the "first line of military support," and to provide early situation and status information to CCDRs and other federal stakeholders. By virtue of its established working relationships with governmental and NGOs at the state/territory and local levels, the NG is in a unique position to serve as a bridge between state/territory/local governmental and NGOs and federal capabilities, including AC forces.

(b) Because the NG remains under the C2 of the state governor until activated under Title 10 USC or otherwise placed into federal service, unique arrangements have been devised to allow NG forces to rapidly transition to a federal status to perform federal missions that need to be conducted under a federal chain of command. For example, the Air Force employment of the NG in support of air defense (AD) missions utilizes "standing orders" that allow ANG forces to automatically transition to Title 10 USC status upon the declaration of an air sovereignty event. This model illustrates that NG forces can be a vital component of a wide range of critical HD operations by executing carefully structured MOAs and other appropriate measures that ensure responsiveness to mission requirements, while preserving the spirit and intent of relevant legal and operational requirements.

(c) With its dual state and federal missions, as well as its community-based presence throughout each state and territory, the NG is uniquely positioned to assist with extension of DOD's HD information environment to the state/territory/local-levels, and to any deployed location throughout the United States and its territories. Both the ARNG and ANG have networks and other information technology services (e.g., e-mail, audio and video teleconferencing, data access, deployable communications systems, etc.) that interconnect all joint force headquarters-state with each other, to ARNG and ANG facilities and organizations nationwide, and to the NGB and beyond. USNORTHCOM and the NGB have jointly pursued strategies to leverage and enhance NG information technology capabilities to bridge gaps and extend the HD information environment to encompass all required levels. These joint planning constructs have been outlined in the separate USNORTHCOM guidance and concept of operations.

b. **State RUF/SRUF**. The state RUF should be reviewed in conjunction with the SRUF to ensure consistency and understanding by the dual status commander.

c. **Geographic Coordinate System**. Federal, state, regional, local, and urban governmental entities use a variety of state and local grid systems and methodologies for specifying geographic locations. This may complicate coordinating activities between federal military units, NG units, and state and local law enforcement and first responders.

d. **USCG**. Although a part of DHS, USCG is a military service and a branch of the Armed Forces of the United States as well as a federal law enforcement agency (Title 14 USC Section 1 and Title 10 USC Section 101). The USCG is at all times an "armed force" under Title 14 USC. The USCG does not require Title 10 USC authority to participate in the national defense of the United States. Upon the declaration of war if Congress so directs in the declaration, or when the President directs, the USCG transfers to the Department of the Navy (Title 14 USC Section 3). Even after transfer, the USCG retains full Title 14 USC

law enforcement authorities. Absent such declaration or direction, the service operates under the auspices of DHS and closely cooperates with the Navy regarding maritime security issues (Title 14 USC Section 145), and assists DOD in the performance of any activity for which the USCG is especially qualified (Title 14 USC Section 141). The USCG plays a vital role in the overall maritime defense of the homeland and is a key player in the maritime HD command and control structure pursuant to the *Memorandum of Agreement Between the Department of Defense and the Department of Homeland Security for the Inclusion of the US Coast Guard in Support of Maritime Homeland Defense*. The *Memorandum of Agreement between the Department of Defense and the Department of Homeland Security for Department of Defense Support to the United States Coast Guard for Maritime Homeland Security* documents capabilities, roles, missions, and functions for DOD support to the USCG and facilitates the rapid transfer of DOD forces to the USCG for support of maritime HS operations. As the federal agency with lead responsibility for maritime HS, the USCG executes the following missions: ports, waterways, and coastal security; maritime threat response and advanced interdiction boardings, drug interdiction; migrant interdiction; defense readiness; civil maritime search and rescue, and other law enforcement.

(1) The USCG has the lead for maritime HS and conducts that under Operation NEPTUNE SHIELD, both within the port and at sea.

(2) The USCG supports tactical law enforcement operations using maritime threat response integrated force packages (IFPs) consisting of tactical law enforcement teams, maritime safety and security teams, the maritime security response team, rotary wing air intercept assets, and supporting lift and surface assets within US ports and waterways, or well forward into the maritime approaches. IFPs conduct intercept, interdiction, and boarding operations within the context of threat response on a graduated scale. USCG assets will conduct operations balancing risk mitigation with evidentiary necessities for further prosecution and intelligence exploitation in support of other federal agencies.

e. **US Air Force Auxiliary**. The Air Force Auxiliary, also known as Civil Air Patrol (CAP), has forces with unique capabilities that can contribute to the successful prosecution of HD air operations. Air Education and Training Command serves as the force provider of CAP to CCDRs. CAP, a volunteer federally chartered nonprofit organization, may function as an auxiliary of the Air Force IAW Title 10 USC Section 9442 to support Air Force noncombatant programs and missions. Such missions may include the use of airborne surveillance and reconnaissance using visual observation and imagery, search and rescue, light airlift, or utilizing CAP aircraft as an "airborne target" during air intercept training.

f. **Posse Comitatus Act (PCA) (Title 18 USC, Section 1385)**. PCA does not apply outside of the homeland. However, if an HD operation transitions to a CS operation, this federal statute, and the court cases that interpret it, places limits on the use of military personnel for civilian law enforcement duties, except as expressly authorized by the Constitution or Act of Congress. Specifically prohibited activities include: interdiction of a vehicle, vessel, aircraft, or similar activity; search and/or seizure; arrest, apprehension, "stop-and-frisk" detentions, and similar activities; and use of military personnel for

surveillance or pursuit of individuals, or as undercover agents, informants, investigators, or interrogators. DODD 5525.5, *DOD Cooperation with Civilian Law Enforcement Officials*, sets forth several forms of assistance to civilian authorities, which are allowed under the PCA. Exceptions to the PCA include:

(1) Support to LEAs under Title 10 USC, Chapter 18;

(2) Presidential directed support under the Enforcement of the Laws to Restore Public Order Act (formerly the Insurrection Act) (Title 10 USC Sections 331-335);

(3) Emergency situations involving WMD (Title 10 USC Section 382);

(4) Prohibited transactions involving nuclear materials (Title 18 USC Section 831).

g. Chapter 18 (Title 10 USC, sections 371-382). This chapter concerns military support for civilian law enforcement agencies and provides statutory authority for specific types of military support to law enforcement. Title 10 USC Section 375 directs SecDef to promulgate regulations that prohibit "direct participation by a member of the Army, Navy, Air Force, or Marine Corps in a search, seizure, arrest, or other similar activity unless participation in such activity by such member is otherwise authorized by law." This guidance is currently set forth in DODD 5525.5, DOD Cooperation with Civilian Law Enforcement Officials.

h. Enforcement of the Laws to Restore Public Order Act (formerly the Insurrection Act, **Title 10 USC, Sections 331 - 335**.) These statutory provisions allow the President, at the request of a state governor or legislature, or unilaterally in some circumstances, to employ the armed forces to suppress insurrection against state authority, to enforce federal laws, or to suppress rebellion.

i. **Critical Infrastructure Protection**. Most infrastructure assets are inherently interconnected and part of larger integrated systems. Therefore, the removal of one asset's functionality due to an outage or attack could have devastating effects on larger infrastructure networks, causing broad service disruptions and potentially adverse regional impacts. Almost all of the national and defense response capabilities rely to some extent on commercial infrastructures. National and DCI supporting national security functions must be available when required to protect our homeland. These will include DCI assets and DIB assets, the protection of which is the responsibility of the DOD. JFCs must be prepared to conduct CIP in either a HD or CS role.

*For complete details on the CS mission, see JP 3-28*, Civil Support.

# APPENDIX B
## KEY INTERAGENCY ORGANIZATIONS

### 1. General

DOD is the lead for HD missions and will be supported by other federal agencies for such missions. Conversely, an agency other than DOD will be supported for CS missions and DOD will play a role in providing that support.

### 2. Combat Support Agencies

CSAs provide direct support to the combatant commands performing HD during wartime or emergency situations and are subject to evaluation by CJCS. Figure B-1 identifies the seven CSAs within DOD. The paragraphs below address general and specific missions, functions, and capabilities of DOD CSAs in support of HD activities.

a. **Defense Information Systems Agency (DISA).** DISA is responsible for planning, engineering, acquiring, fielding, and supporting global net-centric solutions and operating the Defense Information System Network to serve the needs of the President, Vice President, SecDef, and the other DOD components across the range of military operations. DISA supports national security communications requirements and functions within the following core mission areas: communications; C2 capabilities; information assurance (IA); computing services; interoperability, testing, and standards; GIG Enterprise Services; engineering; and acquisition.

*For more information on DISA, see DODD 5105.19, Defense Information Systems Agency (DISA) and its home page at www.disa.mil.*

b. **Defense Intelligence Agency.** DIA is responsible for satisfying military and military related intelligence requirements for SecDef, CJCS, other DOD components, and, as appropriate, non-DOD agencies. With over 7000 military and civilian employees worldwide, DIA is a major producer and manager of foreign military intelligence. It provides military intelligence to warfighters, defense policymakers and force planners in DOD and the IC.

(1) The Director of DIA serves as principal adviser to SecDef and to CJCS on matters of military intelligence. The Director also chairs the Military Intelligence Board that coordinates activities of the defense IC. Moreover, the Director serves as the principal intelligence advisor to ASD(HD&ASA) and the military commands.

(2) With respect to HD, DIA manages DOD warning system that alerts DOD and the USG of potential threats to the nation. DIA's Directorate for Intelligence Production, particularly the Defense Warning Office assesses the most likely developing threats and the high impact threats to military capabilities, and US national infrastructures upon which the military depends for stateside operations, training, and deployment.

(3) DIA's Disruptive Technology Innovations Partnership (DTIP) program provides HD and US infrastructure sectors with actionable information or time-sensitive intelligence assessments for correcting serious vulnerabilities. DTIP assessments prioritize

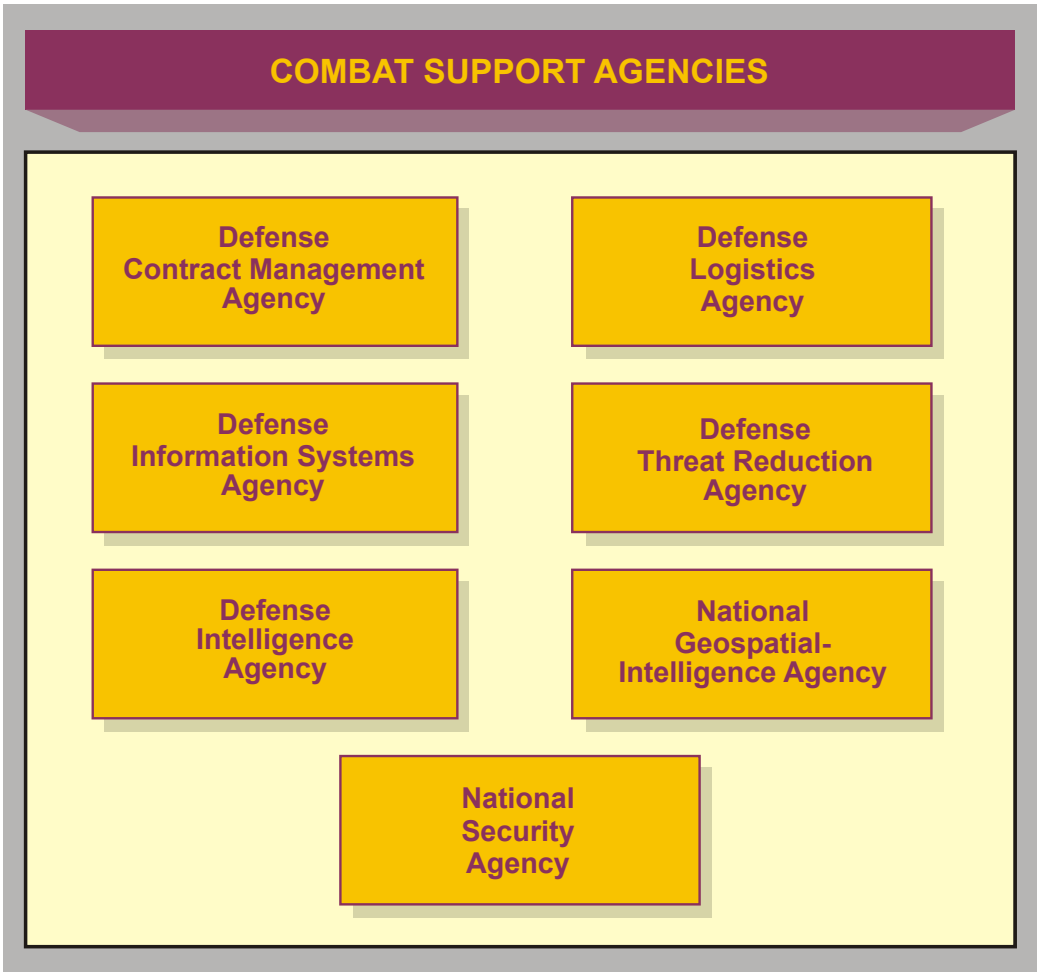



**Figure B-1. Combat Support Agencies**

vulnerabilities according to their national security impact were they to be exploited by state or non-state actors. DTIP assesses and warns of the impact of potential threats stemming from innovative applications of technologies against vulnerabilities.

(4) DIA's Joint Intelligence Taskforce Combating Terrorism is responsible for executing the intelligence component of the DOD campaign against terrorism. It provides warning and threat assessment regarding terrorist activities.

c. **Defense Logistics Agency.** DLA provides worldwide logistic support for the missions of the Military Departments and the combatant commands across the range of military operations. Specifically:

(1) DLA provides logistic support to other DOD components and certain federal agencies, foreign governments, intergovernmental organizations, and others as authorized.

(2) DOD policy states that the primary means of supporting federally declared domestic emergencies is that other federal agencies have the lead and DOD has a supporting role. DLA must be prepared to provide support to CCDRs or other federal agencies.

(3) DLA enhances support to USNORTHCOM in the form of a LNO who works directly with USNORTHCOM J-4, Logistics and Engineering Directorate and through a DLA contingency support team (DCST) when activated. The DLA LNO to USNORTHCOM is the primary focal point for disseminating, coordinating, and tracking USNORTHCOM issues and concerns with DLA. DLA will provide forward-deployed DCSTs (as required) in the USNORTHCOM AOR to meet real-world and contingency requirements within 24 hours after a valid requirement is identified.

(4) *The DLA Customer Handbook*, a reference guide to everything DLA sells and supplies, is available at http://www.dla.mil/J-4/publication.asp#Customer. A toll-free customer number is also available at 1-877-DLA-CALL.

d. **National Security Agency.** The resources of the NSA are organized for the accomplishment of the following missions:

(1) Provides the solutions, products and services that contribute to IA.

(2) The signals intelligence (SIGINT) mission allows for an effective, unified organization and control of all the foreign signals collection and processing activities of the United States. NSA is authorized to produce SIGINT in accordance with objectives, requirements and priorities established by the Director, National Intelligence with the advice of the National Foreign Intelligence Board.

(3) NSA/Central Security Service executes SIGINT and information systems security activities and conducts related activities, as assigned by SecDef, including managing and providing operational control of the US SIGINT System. Executive Order (EO) 12333, *United States Intelligence Activities,* describes in more detail the responsibilities of NSA.

e. **Defense Contract Management Agency (DCMA).** DCMA works directly with defense suppliers to help ensure that DOD, federal, and allied government supplies and services are delivered on time, at projected cost, and meet all performance requirements. DCMA performs all contract audits for DOD and provides accounting and financial advisory services regarding contracts and subcontracts to all DOD components responsible for procurement and contract administration. Within the DCIP, DCMA [subordinate to the Under Secretary of Defense (Acquisition, Technology and Logistics)] is DOD's lead for the defense industrial base sector.

*For more information go to the DCMA webpage at* www.dcma.mil.

f. **National Geospatial-Intelligence Agency.** NGA provides timely, relevant, and accurate geospatial intelligence (GEOINT) in support of national security objectives. GEOINT is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information. Title 10 USC Section 467(5). NGA also:

(1) Supports customers in the defense, law enforcement, intelligence, federal and civil communities with its analytic GEOINT capabilities.

(2) Supports DOD and civil authorities by building integrated datasets to support the COP and situational awareness. These datasets will provide a common frame of reference for federal decision makers and operational planners for critical infrastructure vulnerability analysis and for domestic crisis management (CrM) and CM.

(3) In concert with other federal partners, serves as the imagery and geospatial data broker, integrator, and consolidator in building a single database to support domestic situational awareness, CrM and CM, and CIP.

(4) Provides integrated geospatial information in support of the planning and execution of HD exercises where there is federal, DOD, state and local government participation.

(5) Deploys fully equipped geospatial analytic teams to support military and civilian exercises as well as other crisis and national special security events in real time.

(6) Provides direct, tailored geospatial information support.

(7) Provides externally assigned support personnel as part of the NGA support team (NST) program to combatant commands, Services, intelligence community partners, and civilian agencies such as Department of State, FBI, and DHS. These embedded NST personnel provide day-to-day GEOINT support to the commands or agencies with the capability to reach back to NGA for requirements that exceed the capacity or capability of the team at the command. In addition, NGA maintains a group of support personnel as part of NGA voluntary deployment teams (NVDTs) that can deploy to augment a NST. NST members or individuals from the NVDT can be called upon to participate as part of a national intelligence support team, along with other members of the intelligence community in response to a crisis or emergency situation to augment the staffs of a joint intelligence operations center, command, or agency.

g. **Defense Threat Reduction Agency (DTRA).** DTRA provides services and support to DOD components engaged in war and combating threats to national security. DTRA offers a range of capabilities relating to CBRNE.

(1) DTRA's Operations Center maintains situational awareness and serves as a point of contact for access to a variety of support including:

(a) Secure communications

(b) Technical reach-back for warfighters and first responders, on a 24-hour, 7-day per week basis, in the form of subject matter experts on DTRA computational tools

(c) Video and audio teleconferencing (secure and nonsecure)

(d) Liaison and coordination of assistance from CCDRs and other federal agencies in response to an accident or incident

(e) Exchange of information with other agencies

(f) Technical expertise, advice, and assistance, including targeting

(g) Technical information, including data files on CBRNE materials

(h) Data on effects of radiation on electronics

(i) Modeling/simulation for CBRNE analysis and hazard/consequence prediction. DTRA has the Hazard Prediction and Assessment Capability and Consequence Assessment Tool Set to forecast damage such as blast, heat, radiation, and hazardous material release and the effects of unpredictable phenomena such as natural or manmade disasters

Note: The Interagency Modeling and Assessment Center provides atmospheric hazard predictions in support of the federal response for incidents of national significance.

(j) Information on location and capabilities of specialized DOD and DOE assets capable of responding to accidents or incidents involving radioactive materials

(k) Nuclear forensics for domestic nuclear event attribution

(l) Support to law enforcement investigations

(2) DTRA can deploy the following kinds of support assets:

(a) **Liaison Officers.** While already on-site at certain combatant commands, additional LNOs could be dispatched to other commands as required.

(b) **CM Advisory Teams.** Teams of two to nine experts, including planners, modelers, lawyers, PA specialists, CBRNE specialists, radiation physicians, and health physicists.

(c) **Joint Staff Integrated Vulnerability Assessment Teams.** Assess mission, personnel, and installation vulnerability to terrorist attack.

(d) **Balanced Survivability Assessment Teams.** Assess essential mission systems and critical infrastructure survivability.

(e) **Technical Support Teams.** Provide on-site and direct technical support of DTRA computational tools to warfighters supporting their full spectrum of mission areas.

(f) **Aerial Imagery Collection Support.** Provide leadership and imagery annotation support for joint teams that deploy onboard Air Force OC-135B platforms to collect imagery in support of consequence management.

(3) In addition, DTRA operates the Defense Nuclear Weapons School, which offers a range of courses on WMD topics, with emphasis on nuclear issues.

(4) DTRA is the executive agent for DOD's International Counterproliferation Program. The program works cooperatively with the FBI and DHS to train law enforcement and border security officials of selected countries to investigate, identify, detect, and interdict the illegal transfer of WMD and related materials.

### 3. Other Federal Agencies and Responsibilities

a. **Homeland Security Advisory Council (HSAC).** HSAC provides advice to the President through the Assistant to the President for HS. The Council is advised by four Senior Advisory Committees for HS. The advisory committees include members from state and local government, academia, policy research organizations, the private sector, emergency services, law enforcement, and the public health community. The Council provides advice on:

(1) The development, coordination and implementation of the national strategy to secure the United States from terrorist threats or attacks.

(2) Recommendations to improve coordination, cooperation, and communications among federal, state, and local officials.

(3) The feasibility of implementing specific measures to detect, prepare for, prevent, protect against, respond to, and recover from terrorist threats or attacks.

(4) The effectiveness of the implementation of specific strategies to detect, prepare for, prevent, protect against, respond to, and recover from terrorist threats or attacks.

b. **The Department of Homeland Security**. The Homeland Security Act of 2002 established this department. Figure B-2 shows the organizational structure of DHS. Key directorates, components and the Incident Advisory Council are discussed below.

(1) **The Office of National Protection & Programs** bolsters the nation's security through a multilayered system of preparedness measures based on risk assessment and management. Working with state, local, and private sector partners, the directorate identifies threats, determines vulnerabilities, and targets resources where risk is greatest. Through grants and training on both national and local levels, DHS fosters a layered system of protective measures to safeguard our borders, seaports, bridges and highways, and critical information systems.

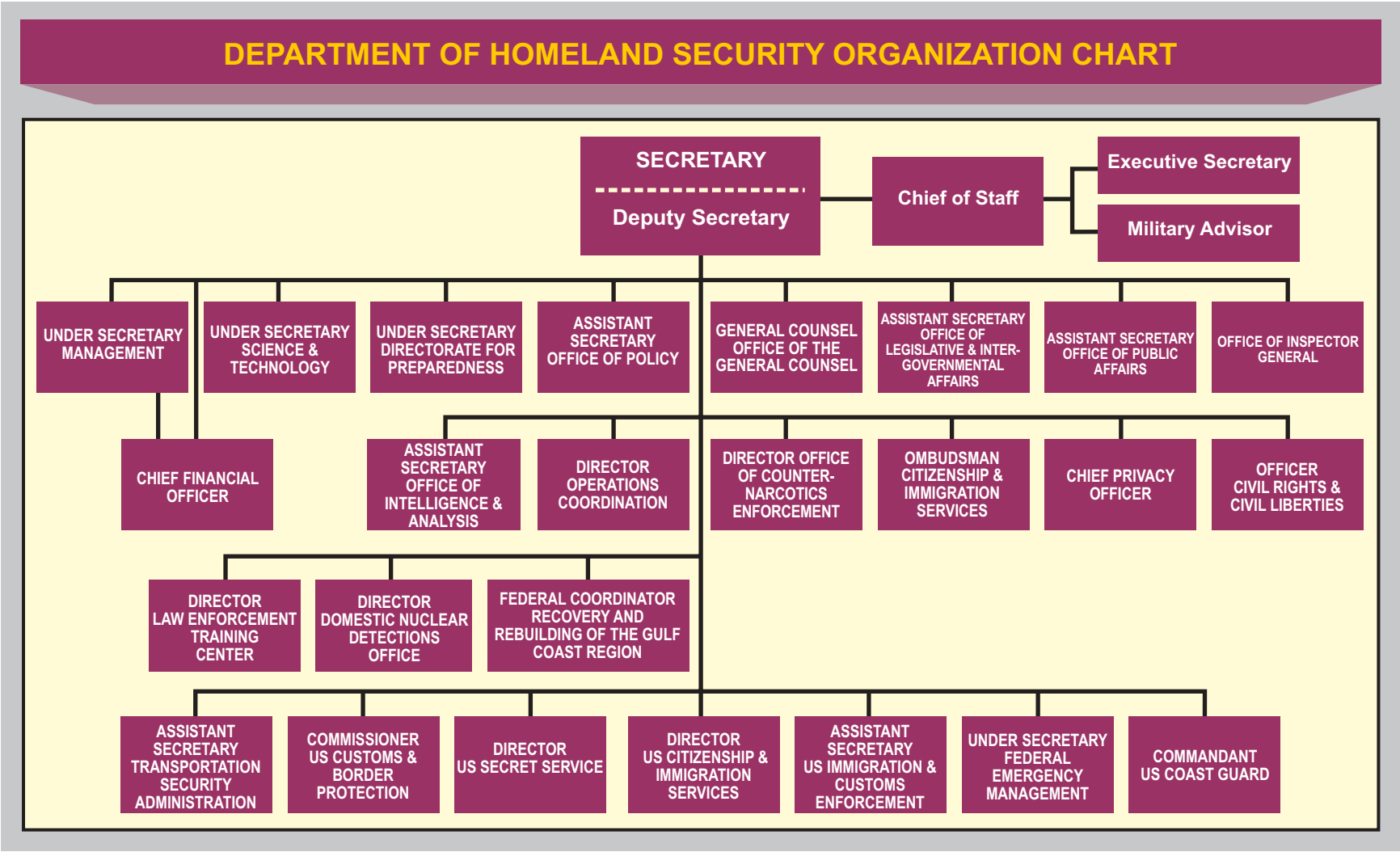



**Figure B-2. Department of Homeland Security Organization Chart**

(2) **The Office of Science and Technology** is the primary research and development arm of DHS. The S&T Directorate provides Federal, state and local officials with the technology and capabilities to protect the homeland.

(3) **The Office of Management** is responsible for budget, appropriations, expenditure of funds, accounting and finance; procurement; human resources and personnel; information technology systems; facilities, property, equipment, and other material resources; and identification and tracking of performance measurements relating to the responsibilities of DHS.

(4) **The Office of Intelligence and Analysis** is responsible for using information and intelligence from multiple sources to identify and assess current and future threats to the United States.

(5) **The Directorate of Operations (Operations Directorate)** is responsible for monitoring the security of the United States on a daily basis and coordinating activities within DHS and with governors, advisors, law enforcement partners, and critical infrastructure operators in all 50 states and more than 50 major urban areas nationwide.

(6) **The Office of Policy** strengthens HS by developing and integrating Department-wide policies, planning, and programs in order to better coordinate DHS's prevention, protection, response and recovery missions.

(7) **The Domestic Nuclear Detection Office (DNDO)** is a jointly staffed office established to improve the Nation's capability to detect and report unauthorized attempts to import, possess, store, develop, or transport nuclear or radiological material for use against the Nation, and to further enhance this capability over time.

(8) **Federal Emergency Management Agency (FEMA)** assists the federal, state and local authorities in preparing for all hazards; manages Federal response and recovery efforts following any national incident, and administers the National Flood Insurance Program.

(9) **Transportation Security Administration (TSA)** protects the nation's transportation systems to ensure freedom of movement for people and commerce.

(10) **Customs and Border Protection** is responsible for protecting our nation's borders in order to prevent terrorists and terrorist weapons from entering the United States, while facilitating the flow of legitimate trade and travel.

(11) **Immigration and Customs Enforcement,** the largest investigative arm of DHS, is responsible for identifying and shutting down vulnerabilities in the nation's border, economic, transportation and infrastructure security.

(12) **Federal Law Enforcement Training Center** provides career-long training to law enforcement professionals to help them fulfill their responsibilities safely and proficiently.

(13) **Citizenship and Immigration Services** is responsible for the administration of immigration and naturalization adjudication functions and establishing immigration services policies and priorities.

(14) **The USCG** protects the public, the environment, and US economic interests—in the nation's ports and waterways, along the coast, on international waters, or in any maritime region as required to support national security.

(15) **The US Secret Service** protects the President and other high-level officials and investigates counterfeiting and other financial crimes, including financial institution fraud, identity theft, computer fraud; and computer-based attacks on our nation's financial, banking, and telecommunications infrastructure."

*For more information on the* Incident Advisory Council*, see the* NRP.

c. **Department of Energy.** DOE serves as a support agency to the FBI for technical operations and a support agency to DHS/FEMA for CM. DOE provides scientific and technical personnel and equipment in support of the federal agency with lead responsibility during all aspects of WMD incidents. DOE assistance can support both CrM and CM activities with capabilities such as threat assessments, domestic emergency support team (DEST) deployment, federal agency with lead responsibility advisory requirements, technical advice, forecasted modeling predictions, and assistance in the direct support of operations. Additionally, DOE provides expertise to the DHS Nuclear Incident Response Team (NIRT) that provides DHS with a nuclear/radiological response capability. When activated, the NIRT consists of specialized federal response teams drawn from DOE and/or Environmental Protection Agency (EPA). These teams may become DHS operational assets providing technical expertise and equipment when activated during a crisis or in response to a nuclear/radiological incident as part of the DHS Federal response. Deployable DOE scientific technical assistance and support includes capabilities such as search operations; access operations; diagnostic and device assessment; radiological assessment and monitoring; identification of material; development of federal protective action recommendations; provision of information on the radiological response; render safe operations; hazards assessment; containment, relocation and storage of special nuclear material evidence; post-incident cleanup; and on-site management and radiological assessment to the public, the White House, and members of Congress and foreign governments. All DOE support to a federal response will be coordinated through a senior DOE official.

d. **DOJ/FBI.** As the lead for CrM and CT, the Attorney General is responsible for ensuring the development and implementation of policies directed at preventing terrorist attacks domestically, and will undertake the criminal investigation and prosecution of acts of terrorism. DOJ has charged the FBI with execution of its lead agency responsibilities for the management of a federal response to threats or acts of terrorism that take place within US territory or those occurring in international waters that do not involve flag vessels of foreign

countries. As federal agency with lead responsibility, the FBI will implement a federal CrM response, and will designate a federal on-scene commander to ensure appropriate coordination with federal, state and local authorities until such time as the Attorney General finds it necessary to transfer the overall lead to DHS/FEMA.

e. **Department of Transportation / Federal Aviation Administration**. The mission of DOT is to serve the United States by ensuring a fast, safe, efficient, accessible and convenient transportation system that meets our vital national interests and enhances the quality of life of the American people. It provides air movement and flight plan data for all commercial and other aircraft operations that are critically important in determining if any aircraft are deviating from normal planned flight operations. The FAA, under DOT, oversees the safety of civil aviation and maintains primary jurisdiction over all air space within the US National Airspace System. In close coordination with DOD and NORAD, FAA clears air traffic as need to expedite intercept operations. The safety mission of the FAA is first and foremost and includes the issuance and enforcement of regulations and standards related to the manufacture, operation, certification and maintenance of aircraft. The agency is responsible for the rating and certification of airmen and for certification of airports serving air carriers. It also regulates a program to protect the security of civil aviation, and enforces regulations under the Hazardous Materials Transportation Act for shipments by air. The FAA, which operates a network of airport towers, air route traffic control centers, and flight service stations, develops air traffic rules, allocates the use of airspace, and provides for the security control of air traffic to meet national defense requirements. Other responsibilities include maintaining most of the radars performing air surveillance over the CONUS FAA control centers, providing cueing for targets of interest, and providing maintenance and logistics support for nearly all ground to air radios used by the air defense sectors. These and other support activities and procedures are governed by a series of agreements and FAA orders pursuant to a capstone National Agreement -120.

f. **Environmental Protection Agency.** EPA serves as a support agency to the FBI for technical operations, and a support agency to DHS/FEMA for CM. In certain situations, the EPA may also act in a lead role IAW Comprehensive Environmental Response, Compensation, and Liability Act (Superfund). EPA provides technical personnel and supporting equipment to the federal agency with lead responsibility during all aspects of WMD incidents. EPA assistance may include threat assessment; DEST and regional emergency response team deployment; advice to the federal agency with lead responsibility, technical advice, and operational support for chemical, biological, and radiological releases; consultation; agent identification; hazard detection and reduction; environmental monitoring; sample and forensic evidence collection/analysis; identification of contaminants; feasibility assessment; clean-up; and on-site safety, protection, prevention, decontamination, and restoration activities. EPA and USCG share responsibilities for response to oil discharges into navigable waters and releases of hazardous substances, pollutants, and contaminants into the natural and physical environment. EPA provides the predesignated federal on-scene coordinator for inland areas while USCG coordinates resources for the containment, removal, and disposal activities and resources during an oil, hazardous substance, or WMD incident in coastal areas.

g. **Department of Health and Human Services.** DHHS assistance supports threat assessment, DEST deployment, epidemiological investigation, advice to the federal agency with lead responsibility, and technical advice. Technical assistance to the FBI may include identification of agents, sample collection and analysis, on-site safety and protection activities, and medical management planning. DHHS serves as a support agency to the FBI for technical operations, and a support agency to DHS/FEMA for CM. DHHS provides technical personnel and supporting equipment to the federal agency with lead responsibility during all aspects of an incident. DHHS can also provide regulatory follow-up when an incident involves a product regulated by the Food and Drug Administration. Operational support to DHS/FEMA may include mass immunization, mass prophylaxis, mass fatality management, pharmaceutical support operations (Strategic National Stockpile), contingency medical records, patient tracking, and patient evacuation and definitive medical care provided through the National Disaster Medical System. In the event of a CS operation simultaneous to a HD event, the DHHS is the federal agency with lead responsibility for Emergency Support Function 8, Public Health and Medical Service. DHHS monitors blood availability and maintains contact with the American Association of Blood Banks Inter-organizational Task Force on Domestic Disasters and Acts of Terrorism, of which the ASBPO is a member.

h. **US Department of Agriculture (USDA).** USDA serves as the primary support agency to DHS/FEMA for disaster relief and CM for firefighting, food, and agro-terrorism issues. USDA, through the US Forest Service, manages and coordinates firefighting activities by providing personnel, equipment, and supplies in support of state and local agencies involved in firefighting operations. During major disasters and emergencies, USDA is responsible for identifying food assistance required, securing needed supplies, and arranging for the transportation of food assistance to affected areas requiring emergency rations.

i. **General Services Administration (GSA).** GSA serves as the primary support agency to DHS/FEMA for resource support during disaster relief and CM operations. GSA provides emergency supplies, space, office equipment, office supplies, telecommunications, contracting services, transportation services, and security services through its contracting authorities.

j. **American Red Cross.** The American Red Cross serves as the primary support agency to DHS for coordinating mass care support with other NGOs during disaster relief and CM operations. Support may include shelter, feeding, emergency first aid, disaster welfare information, bulk distribution, supportive counseling, blood, and blood products.

Intentionally Blank

# APPENDIX C
# NORTH AMERICAN AEROSPACE DEFENSE COMMAND MISSIONS, ORGANIZATION, AND STRUCTURE

*"NORAD is the cornerstone of our air defense capability. Our air defense success rests on an integrated system for air surveillance and defense against air threats at all altitudes."*

**Strategy for Homeland Defense and Civil Support**
**June 2005**

## 1. North American Aerospace Defense Command Overview

a. Since 1958, Canada and the United States have defended the skies of North America through NORAD, a binational command. Using data from satellites, as well as airborne and ground-based radars, NORAD monitors, validates, and warns of attack against the Canadian and US homelands by aircraft, missiles, and space vehicles; symmetric as well as asymmetric threats. The command ensures Canadian and US air sovereignty through a network of alert fighters, tankers, airborne early warning aircraft, and ground-based air defense assets cued by military and interagency surveillance radars, such as those of the FAA and its Canadian equivalent, NAV CANADA. Since the unexpected historic events of 9/11/01, NORAD has made significant changes – primarily from looking only outward, toward suspected threats, to additionally monitoring both maritime and aerospace threats in the approaches, inland waterways, and internal air space of the United States and Canada.

b. As a properly executed international covenant, the NORAD Agreement is binding under international law. The Canadian Chief of Defence Staff (CDS) and the US CJCS provide the Terms of Reference to the NORAD Agreement to supplement and clarify military responsibilities directed or implied by the Agreement.

c. In the context of NORAD's missions, "North America" means Alaska, Canada, the CONUS, Puerto Rico and the US Virgin Islands, to include the Air Defense Identification Zone, the air approaches, maritime approaches and territorial seas, and the internal navigable waterways (principally the Gulf of St. Lawrence, St. Lawrence Seaway System, Great Lakes and other internal waterways of concern as identified by CDRNORAD). Responsibility for aerospace warning and aerospace control of US territory outside North America (e.g., Hawaii and Guam) lies with the appropriate combatant commander.

**The 2006 NORAD Agreement Establishes Three Primary Missions For NORAD:**

**a. Aerospace Warning for North America.**
**b. Aerospace Control for North America.**
**c. Maritime Warning for North America.**

**NORAD Agreement Terms of Reference**

## 2. Missions

a. **Aerospace Warning** consists of processing, assessing, and disseminating intelligence and information related to man-made objects in the aerospace domain and the detection, validation, and warning of attack against North America whether by aircraft, missiles or space vehicles, utilizing mutual support arrangements with other commands and agencies. An integral part of aerospace warning entails monitoring of global aerospace activities and related developments. NORAD's aerospace warning mission for North America includes support of United States commands that are responsible for missile defense.

b. **Aerospace Control** consists of providing surveillance and exercising OPCON of the airspace of the United States and Canada. OPCON is the authority to direct, coordinate, and control the operational activities of forces assigned, attached, or otherwise made available to NORAD.

c. **Maritime Warning** (new mission tasking per the 2006 NORAD Agreement) consists of processing, assessing, and disseminating intelligence and information related to the respective territorial seas and internal waterways of, and the maritime approaches to, the United States and Canada, and warning of maritime threats to, or attacks against North America utilizing mutual support arrangements with other commands and agencies responsible for maritime defense and security. Through these tasks, shall develop a comprehensive shared understanding of maritime activities to better identify potential maritime threats to North American security. Maritime surveillance and control shall continue to be exercised by national commands and, as appropriate, coordinated bilaterally.

## 3. Supporting Mission Areas and Systems

a. **Integrated Tactical Warning and Attack Assessment (ITW/AA).** The essence of the aerospace warning and control missions is embodied in the command's ITW/AA responsibilities. Integrated tactical warning is defined as warning after initiation of a strategic or tactical aerospace threat event based on an evaluation of information from all available sources. Attack assessment is defined as an evaluation of information to determine the potential or actual nature and objectives of an aerospace attack for the purpose of providing information for timely decisions. The ITW/AA system is a critical component of the US nuclear C2 system and is comprised of the sensors, command centers, and communications networks required to detect, assess and communicate its information to designated users. **The main purpose of the ITW/AA system is to provide timely, reliable, and unambiguous warning information of ballistic missile, space and air attacks on North America.** To provide ITW/AA of an aerospace attack on North America, NORAD, as a supported command, correlates and integrates relevant information. Space surveillance, nuclear detonation detection and ballistic missile warning information is provided by USSTRATCOM for NORAD to execute its aerospace warning mission for North America. CDRUSSTRATCOM, as a supporting commander retains OPCON over USSTRATCOM-assigned ballistic missile and space surveillance and warning systems, the

Nuclear Detonation Detection System, and command, control and communications systems. CDRNORAD retains the authority to redirect operational priorities of the ITW/AA systems to execute NORAD assigned missions in accordance with the priority assigned to attacks against North America.

b. **Routine Air Operations.** NORAD is responsible for providing surveillance and control of North American airspace, this includes:

(1) Day-to-day surveillance and control of the airspace approaches to and the airspace within North America to safeguard the sovereign airspace of both Canada and the United States.

(2) Surveillance and control includes the capability to detect, identify, monitor and, if necessary, take appropriate actions (ranging from visual identification to destruction) against manned or unmanned air-breathing vehicles approaching North America.

(3) In times of crisis or war, air defense against manned or unmanned air-breathing weapon systems attacking North America

c. **Information and Intelligence Sharing.** NORAD aerospace warning, maritime warning and aerospace control missions require effective information and intelligence sharing by many organizations and agencies within Canada and the United States. A "need to share" philosophy facilitates the effective execution of these NORAD missions on behalf of the governments of Canada and the United States.

d. **Interagency Cooperation.** The effective execution of NORAD missions requires significant cooperation with agencies outside of the Department of National Defence (NDHQ) in Canada and the DOD in the United States. NORAD is authorized direct liaison with these agencies in order to solicit and acquire the necessary cooperation, while keeping appropriate national commands and authorities informed.

e. **NORAD, Canada Command (Canada COM) and US Northern Command.** NORAD supports Canada COM and USNORTHCOM in their assigned missions to defend Canada and the United States. NORAD is supported by both commands in the conduct of missions assigned to NORAD. NORAD provides binational situation awareness of the aerospace and maritime domains to Canada COM and USNORTHCOM.

*"Close cooperation, liaison, and intelligence and information sharing among these commands will ensure the ability of our armed forces to act, in a timely and coordinated fashion, to deter, identify, disrupt and defeat threats to Canada and the United States"*

**CANUS Basic Defense Document**
**July 2006**

f. **Information Operations.** NORAD conducts IO on an ongoing basis to achieve and maintain information superiority while enhancing deterrence. NORAD plans,

coordinates and directs IO as delineated in each nation's IO doctrine. Operations are primarily defensive in nature. However, in consultation with each national authority, actions can be directed to safeguard information superiority and NORAD's ability to execute its assigned missions.

g. **Direct Communications.** CDRNORAD is authorized direct communications with the CDS and the CJCS and with Commander, Canada COM, CDRUSNORTHCOM, CDRUSPACOM, CDRUSSTRATCOM, CDRUSSOUTHCOM, and other commanders on matters of HD interest. This includes requests to appropriate agencies to expedite the release of classified information to facilitate the accomplishment of NORAD's missions.

h. **Conference Calls.** NORAD uses a series of telephonic conferences as a secure means of rapidly sharing information among combatant commands and other organizations and to inform and alert senior military and government leadership of a developing situation. The purposes of these telephonic conferences is to improve the situational awareness of all concerned organizations, to increase the time available for senior leadership to make informed decisions and finally to increase the time available for NORAD and other military forces and civil agencies to respond to the situation at hand.

i. **Counterdrug (CD) Operations.** The aerial and maritime transit of illegal drugs into North America has been identified as a threat to the national security of Canada and the United States by both governments. To counter this threat, the 1989 National Defense Authorization Act assigned DOD as the federal agency with lead responsibility in the detection and monitoring of illegal airborne and maritime drug trafficking into the United States. To accomplish this mission the SecDef tasked CDRNORAD and selected combatant commanders to conduct detection and monitoring operations. Likewise, the Canadian National Drug Strategy named the NDHQ as a supporting department to the Royal Canadian Mounted Police. As a result, 1 Canadian Air Division is responsible for conducting CD operations when directed by the NDHQ. To accomplish this mission, NORAD conducts operations to detect and monitor aerial transit of drug trafficking into North America; coordinates with other federal, provincial, state and local agencies engaged in detecting, monitoring and apprehending aerial drug traffic; and integrates NORAD operations into an effective CD network.

*It is important to understand the differences between Canadian and US law with regard to military support to LEAs. NORAD Instruction 10-24 provides additional detail on this subject and should be consulted by those planning or executing CD activities for NORAD.*

## 4. North American Aerospace Defense Command Organization

NORAD is organized on three distinct levels. The Headquarters NORAD staff and the Command Center operate at the **"strategic"** level. The three NORAD regions conduct activities at the **"operational"** level and the air defense sectors and their TACON forces operate at the **"tactical"** level. CDRNORAD conducts operations through or with the support from the elements shown in Figure C-1.

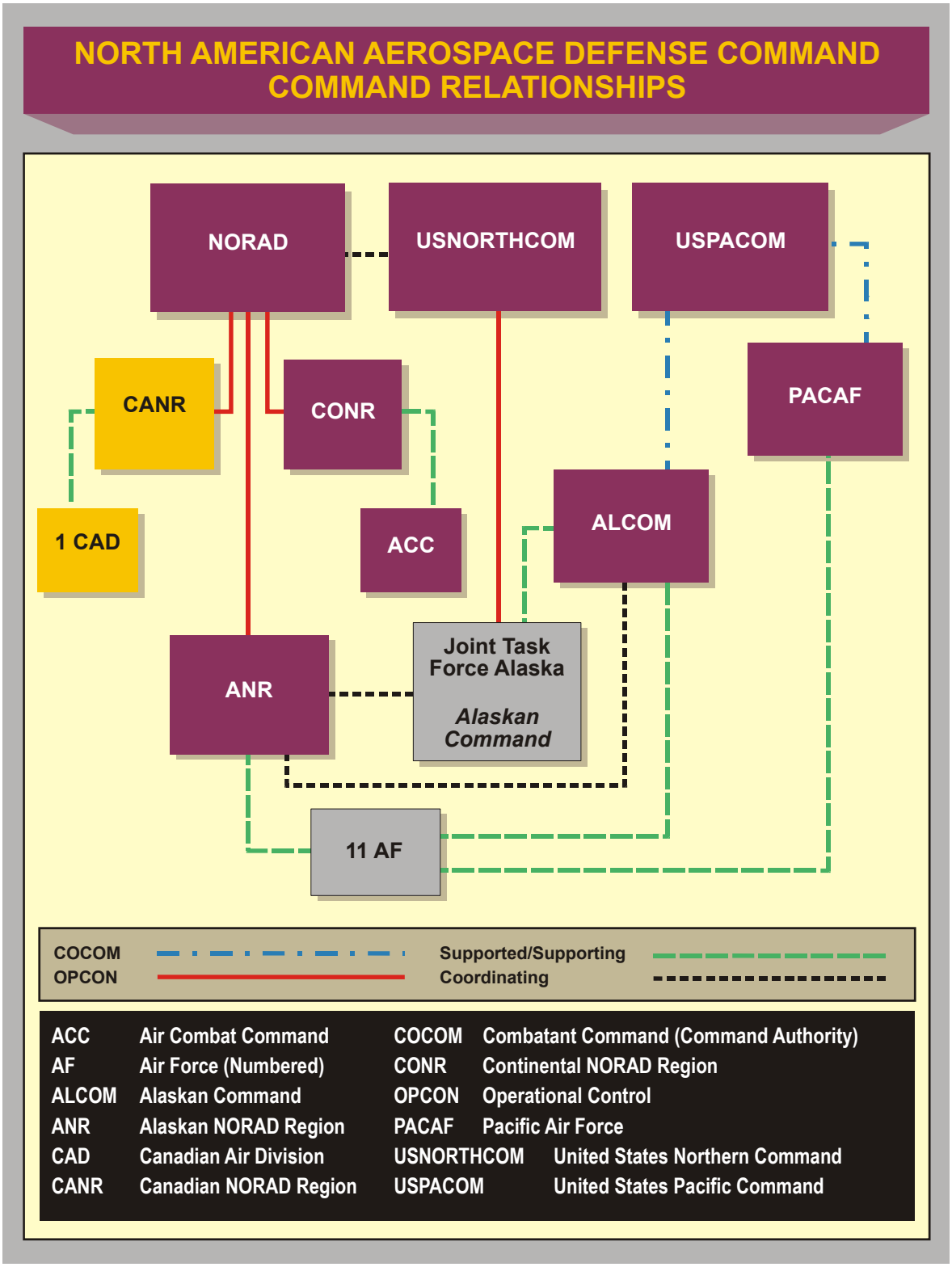



**Figure C-1. North American Aerospace Command Command Relationships**

a. Missions are accomplished through a combination of assigned and attached Canadian and US forces (AC, National Guard, and reserves). These forces are employed in three NORAD regions, further described in paragraph 6.b.

(1) **Commander NORAD.** CDRNORAD and the Deputy Commander (ND NORAD) cannot be from the same country, and their appointments must be approved by both the Canadian and the US governments. The jurisdiction of CDRNORAD over those forces specifically made available to NORAD by the two governments is limited to "OPCON," which is defined as the authority to direct, coordinate, and control the operational activities of forces assigned, attached or otherwise made available.

(2) **Commander US Element NORAD (CDRUSELEMNORAD).** CDRUSELEMNORAD is the senior US officer assigned to NORAD. US Element NORAD (USELEMNORAD) serves as an administrative construct to permit the assignment of US forces to perform NORAD missions. Global Force Management Guidance Section II, Assignment of Forces (Forces For Unified Commands) states, "Although not a combatant commander, Commander, United States Element North American Aerospace Defense Command (CDRUSELEMNORAD), exercises COCOM over US forces made available to NORAD".

(3) Headquarters **NORAD.** Headquarters NORAD, through the NORAD – USNORTHCOM Command Center, provides the strategic guidance necessary for the regions to execute their assigned missions. Additionally, the headquarters coordinates with the senior military staffs of both countries as well as other combatant commanders who may be in a supporting role. Headquarters NORAD and the command centers must be composed of integrated staffs with representatives of both countries.

(4) Headquarters **NORAD Staff Organization**. The Headquarters NORAD staff is organized along the traditional US joint staff J-code construct. In addition, the commander's staff includes both Canadian and US political advisors, an interagency group, a Washington Office, and special assistants for NG and reserve affairs. A unique aspect of the Headquarters NORAD staff is that all these staff elements are "dual-hatted" as both NORAD and USNORTHCOM organizations, with the exception of the operations directorate (J-3), which is a NORAD-only organization. Despite the fact that the majority of the staff is "dual-hatted" with USNORTHCOM, the commands are separate with complementary missions, roles and responsibilities.

## 5. North American Aerospace Defense Command Relations With Other Commands

a. **United States Northern Command.** NORAD and USNORTHCOM share a special and unique relationship. A majority of USNORTHCOM's AOR and NORAD's OA overlap as indicated in Figure C-2 (note that in the NORAD Agreement this is normally referred to as an "AO"). Each command has its missions defined by separate sources. NORAD is a binational military organization which exists under the authority of the North Atlantic Treaty and the NORAD Agreement, The NORAD Agreement Terms of Reference, and the Canada-US (CANUS) Basic Defense Document between Canada and the United States. Conversely, USNORTHCOM is a purely US military organization based on the US UCP. Specific support and coordination between NORAD and USNORTHCOM include:

(1) USNORTHCOM forces operating in the same area as NORAD forces may provide collateral support by giving tactical intercept information and control to NORAD forces. Conversely, NORAD air defense control assets may provide tactical intercept information and control to USNORTHCOM forces while they remain under the OPCON of their respective commander.

(2) USNORTHCOM coordinates with NORAD for the air defense of and maritime approaches to North America and support to civil authorities, to include drug interdiction.


**Figure C-2. North American Aerospace Defense Command Operational Area**

(3) In conjunction with USPACOM, via ALCOM and Army Pacific, USNORTHCOM coordinates with NORAD for the ground defense of Alaska.

(4) USNORTHCOM coordinates with NORAD for the ground defense of CONUS.

(5) In conjunction with the Canadian Chief of Maritime Staff, USNORTHCOM coordinates with NORAD for the defense of maritime approaches to North America including air defense coordination**.**

*"NORAD and USNORTHCOM are two separate commands. Neither command is subordinate to the other or a part of the other, but work very closely together. Members of the two commands work side-by-side…and, in many cases, United States military members are dual-hatted in positions on both staffs."*

**General Ralph E. Eberhart**
**Testimony before the House Armed Services Committee**
**March 2003**

b. **United States Strategic Command.** USSTRATCOM support to NORAD includes the following:

(1) Provide the missile warning and space surveillance information necessary to fulfill the US commitment to the NORAD Agreement.

(2) Provide ITW/AA of space, missile and air attacks on CONUS and Alaska if NORAD becomes unable to accomplish the aerospace warning mission.

(3) Coordinate with NORAD to support accomplishments of both commands' missions during crisis and war.

c. **United States Transportation Command.** USTRANSCOM provides common-user and commercial air, land and sea transportation, terminal management and aerial refueling to support the global deployment, employment, sustainment, and redeployment of US forces. As such, USTRANSCOM is responsible for the following support to NORAD:

(1) Provide air-refueling support to NORAD, as required. Ensure refueling at forward operating locations and main operating bases are capable of supporting designated operations.

(2) Support NORAD deployment, resupply, and redeployment with air, sea and assets, as directed by the SecDef.

(3) Coordinate force movement requirements and related materials (including strategic aeromedical evacuation) involving common user lift.

d. **United States Pacific Command.** USPACOM's AOR and NORAD's OA overlap. As a result, NORAD entered into a memorandum of understanding (MOU) with USPACCOM to address issues of mutual concern; listing support rendered by one party to the other and to deconflict their operations, when necessary.

e. **United States European Command (USEUCOM).** USEUCOM's AOR extends across the Atlantic Ocean to the west coast of Greenland and east of approximately 45 degrees West longitude. Accordingly, NORAD's OA and USEUCOM's AOR overlap.

f. **United States Southern Command.** NORAD's OA and USSOUTHCOM's AOR overlap. NORAD has an MOU with USSOUTHCOM to address issues of mutual concern, to list support rendered by one party to the other and to deconflict their operations when necessary. Of particular interest to NORAD, this MOU addresses CD operations and US military operations in the vicinity of Cuba.

### 6. North American Aerospace Defense Command Subordinate Commands

a. All NORAD air sovereignty and air control operations are conducted by its subordinate NORAD regions. The individual regions are the "warfighters" and function at the operational and tactical levels of war. Each region is further subdivided into one or more air defense sectors (ADSs). The ADS is responsible for tactical execution of the NORAD missions through detection, identification and required tactical response. The ADS also provide the C2 node for coordination to higher headquarters, either their parent region or NORAD.

b. Each ADS is divided into two functional areas: a battle staff and the sector air operations center (SAOC). When formed, the battle staff directs sector/region air sovereignty and air control activities. Additionally, it directs and coordinates activities of subordinate radar units, relays instructions from senior NORAD elements to subordinate and lateral units and coordinates allocation and employment of air defense resources. The battle staff is assigned or allocated air defense resources (e.g., interceptors, airborne warning and control system or tankers) that are necessary to defend its assigned OA.

c. The SAOC is tasked to support the NORAD mission and operates on a continuous basis. It is the focal point for the conduct of weapons, surveillance, identification and interface control functions. All fighter, tanker, airborne early warning and military radar sites are assigned to an air defense sector for operational and tactical control. The ADS controls the air battle while managing their tactical assets to include both aircraft and surveillance equipment, such as ground-based radars and tethered aerostat balloons. Each SAOC closely coordinates air sovereignty activities with FAA air traffic control centers to ensure HD activities can be safely and successfully executed.

d. The tactical level of NORAD also includes ground based air defense units in certain locations such as the NCR and under certain circumstances, such as a national special security event. Such units report directly to the region and share air picture information with their associated ADS. A geographic depiction of NORAD's regions and

sectors is provided at Figure C-2. A more detailed description of each of the three NORAD regions is provided below.

(1) **Alaskan NORAD Region.** ANR is the binational organization responsible for performing the NORAD air sovereignty and air control mission over the state of Alaska as well as the northwest approaches to North America. HQ ANR is collocated at Elmendorf Air Force Base (AFB), Alaska with HQ ALCOM, a subunified command of USPACOM and JTF-AK a subordinate unit of USNORTHCOM. The ANR Commander is also the Commander of ALCOM, and JTF-AK. ANR is supported by both active duty Canadian forces and US forces, as well as Alaska Air National Guard units. The ANR's Regional Air Operations Center is manned by both US personnel and Canadian forces to maintain continuous surveillance of its OA. The Alaska Air Defense Sector is the single ADS within the ANR and is collocated at Elmendorf AFB.

(2) **Canadian NORAD Region (CANR).** CANR is the binational organization responsible for performing NORAD's air sovereignty and air control mission over Canada as well as the polar approaches to North America. CANR is located at Canadian Forces Base (CFB) Winnipeg, Manitoba. The SAOC for Canada is located at CFB North Bay, Ontario. The CANR Commander is also the Commander of 1 Canadian Air Division (CAD). CANR is manned by both 1 CAD and US personnel.

(3) **Continental United States NORAD Region (CONR).** CONR is the subordinate, binationally staffed command responsible for the air sovereignty and air control of the airspace over the CONUS, to include the approaches to North America. The CONR Commander exercises OPCON over all air defense forces within CONUS from Tyndall AFB, Florida. Air Combat Command (ACC) and USJFCOM are the force providers for ground, sea, and air units apportioned through the Joint Strategic Capabilities Plan (JSCP) to support the NORAD missions. ANG support is liaised through USJFCOM and ACC. CONR operates in an extremely complex, binational and multi-command environment where political, military and economic conditions interrelate. CONR is collocated with a numbered air force subordinate to ACC. The CONR Commander is also the Commander, AFNORTH, located at Tyndall AFB, Florida, and may be designated the JFACC for USNORTHCOM for unilateral US air operations within the USNORTHCOM AOR. CONR ADSs are identified below:

(a) **CONR ADSs and the National Capital Region Integrated Air Defense System (NCR – IADS) are identified below.** NCR-IADS is a unique sub-element of CONR, which was established in response to terrorist air threats to the NCR. NCR-IADS is OPCON to CONR and has a coordination relationship with Eastern Air Defense Sector (EADS).

(b) **Eastern Air Defense Sector (EADS).** EADS, located in Rome, New York is the binational SAOC responsible for all CONR operations east of 97 degrees West Longitude.

(c) **Western Air Defense Sector (WADS)**. WADS, located at McChord AFB, Washington, is the SAOC responsible for all CONR air operations west of 97 degrees West Longitude (roughly the Mississippi River).

## 7. Other Forces

a. **US Element NORAD.** USELEMNORAD is an organizational construct created in response to the requirements of Title 10 USC that specifies that US military forces must be kept in a US military "chain-of-command", and may not be assigned directly to a multinational, or binational command. CDRUSELEMNORAD is the senior US officer assigned to NORAD

b. **First Canadian Air Division.** Winnipeg, Manitoba is home to the dual headquarters for 1 CAD and the CANR. The headquarters serve as the central point of C2 for Canada's operational Air Force and oversees the monitoring of Canada's airspace in support of commitments to the NORAD.

## 8. North American Aerospace Defense Command Regulations and Operating Instructions

Details on the NORAD processes and procedures for any of its particular mission areas are documented in the various NORAD instructions published by the Command. These documents are to be considered directive for all NORAD personnel both at the headquarters and subordinate units. A complete list of these documents is maintained on the NORAD portal on the Non-secure Internet Protocol Router Network (NIPRNET) (www.noradnorthcom.mil). Content of classified NORAD instructions may be found on the classified releasable to Canada (RELCAN) and SECRET Internet Protocol Router Network (SIPRNET) networks.

Intentionally Blank

# APPENDIX D
## KEY HOMELAND DEFENSE LEGAL AND POLICY DOCUMENTS

### 1. Legal and National Policy and Guidance

There are a variety of documents that provide guidance for the HD mission. These range from the US Constitution to CJCSIs.

a. **The Constitution.** The Preamble states that two of the purposes of the Constitution are to ensure domestic tranquility and provide for the common defense. Furthermore, Congress has the power to declare war, raise and support armies, provide and maintain a Navy, and provide for calling forth the militia to execute the laws of the Union, suppress insurrections, and repel invasions. The President is the Commander in Chief of the Armed Forces. The Constitution provides the basis for HD through the guarantee of domestic tranquility and provision for the common defense of the nation.

b. **Key Executive and Legislative Guidance.** The following documents are key references when addressing HD operations:

(1) Title 10 USC (Armed Forces). Title 10 USC provides guidance on the Armed Forces of the US. Guidance is divided into five subtitles. One on general military law and one each for the US Army, USN and US Marine Corps, the US Air Force and the Air Force Auxiliary (Civil Air Patrol), and the Reserve Components.

(2) Titles 14, 33, 46 and 50, USC. These statutes define the statutory authority for the USCG to conduct HD and HS missions.

(3) Title 32 USC, *National Guard*. Title 32 defines the organization, personnel, training, and equipping of the NG. Additionally, Title 32 USC provides the authority to allow for the NG to conduct HD activities under state C2 and for a NG commander to retain his/her state commission (Title 32 USC) after ordered to active duty (Title 10 USC) allowing for a "dual-hat" commander to ensure unity of effort for state and federal military forces.

(4) Title 50 USC, *War and National Defense*. Title 50 provides guidance on war and national defense. Among the major provisions of Title 50 are: Establishes a Council of National Defense to coordinate industries and resources for national security; authorizes the detention and removal of individuals from foreign nation(s) with which the United States is at war; authorizes financial reward for information concerning the illegal introduction, manufacture, acquisition, export or conspiracies concerning special nuclear material or atomic weapons; and regulations for the anchorage and movement of vessels during national emergency. Other major provisions of Title 50: Addresses insurrection; definition and declaration of national security; air warning and defense; internal security and subversive activities; national defense contracts; chemical and biological warfare programs; war powers resolution and definition of national emergencies; international emergency economic powers; foreign intelligence surveillance; and defense against WMD.

(5) HSPD-1, *Organization and Operation of the Homeland Security Council.* HSPD-1 established the Homeland Security Council to ensure coordination of all HS-related

activities among the executive departments and agencies and promote the effective development and implementation of all HS policies.

(6) HSPD-2, *Combating Terrorism Through Immigration Policies.* HSPD-2 established policies and procedures to prevent aliens who engage in or support terrorist activity from entering the United States and to detain, prosecute, or deport any such aliens who are within the United States.

(7) HSPD-3, *The Homeland Security Advisory System.* HSPD-3 provides the guidelines for a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to federal, state and local authorities and the American people. This document establishes the five threat conditions and their respective protective measures.

(8) HSPD-4/NSPD-17, *National Strategy to Combat Weapons of Mass Destruction.* HSPD-4 states that nuclear, biological, and chemical weapons in the possession of hostile states and terrorists represent one of the greatest security challenges facing the United States and that we must pursue a comprehensive strategy to counter this threat in all of its dimensions. It describes three pillars for our national strategy to combat WMD: counterproliferation to combat WMD use, strengthen nonproliferation to combat WMD proliferation, and CM to respond to WMD use. Each pillar iterates specific actions to be pursued within the pillar.

(9) HSPD-5, *Management of Domestic Incidents*. Assigns the Secretary HS as the principal federal official for domestic incident management to coordinate the federal government's resources utilized in response to, or recovery from terrorist attacks, major disasters, or other emergencies. The federal government assists state and local authorities when their resources are overwhelmed, or when federal interests are involved. Nothing in the directive impairs or otherwise affects the authority of SecDef over DOD, including the chain of command for military forces. SecDef provides civil support for domestic incidents as directed by the President. SecDef retains command of military forces providing CS. Additionally, HSPD-5 directed the development of a National Incident Management System to provide a consistent nationwide approach for federal, state, local and tribal governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents. It also directed the development of a National Response Plan (NRP) to provide a unified approach for coordinating the federal, state, and local response to an incident of national significance.

(10) HSPD-6, *Integration and Use of Screening Information*. HSPD-6 provides for the development and maintenance of accurate and current information about individuals known or appropriately suspected to be or have been engaged in conduct related to terrorism; and that information, as appropriate and permitted by law, can be used to support screening and protective processes via the Terrorist Screening Center.

(11) HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection.* HSPD-7 established a national policy for federal departments and agencies to identify and prioritize US critical infrastructure and key resources and to protect them from terrorist

attacks. This directive identifies roles and responsibilities of the Secretary of Homeland Security, and other departments and recognizes DOD as the sector-specific agency for the defense industrial base.

(12) HSPD-8, *National Preparedness*. HSPD-8 established policies to strengthen US preparedness to prevent and respond to threats and actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of federal preparedness assistance to state and local governments, and outlining actions to strengthen preparedness capabilities of federal, state, and local entities.

(13) HSPD-10/NSPD-33, *Biodefense for the 21st Century*. HSPD-10 provides a comprehensive framework for US biodefense and, among other things, delineates the roles and responsibilities of federal agencies and departments in continuing their important work in this area.

(14) HSPD-11, *Comprehensive Terrorist-Related Screening Procedures*. HSPD-11 establishes procedures to enhance terrorist-related screening through comprehensive, coordinated procedures that detect, identify, track, and interdict people, cargo, conveyances, and other entities and objects that pose a threat to HS.

(15) HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors.* HSPD-12 establishes a policy of the United States to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors.

(16) HSPD-13/NSPD-41, *Maritime Security Policy*. HSPD-13 establishes US policy, guidelines, and implementation actions to enhance US national security and HS by protecting US maritime interests.

(17) HSPD-14/NSPD-43, *Domestic Nuclear Detection Office*. HSPD-14 establishes the Domestic Nuclear Detection Office (DNDO) resident within the DHS and assigns it with the responsibility to develop the global nuclear detection architecture and to acquire and support the deployment of the domestic detection system and directs DOD to conduct close cooperation and coordination with the DNDO.

(18) NSPD-1, *Organization of the National Security Council System. N*SPD-1 established the national Security Council system as a process to coordinate executive departments and agencies in the effective development and implementation of those national security policies.

(19) HSPD-16/NSPD-47 *US Aviation Security Policy*. The US Aviation Security Policy establishes US policy, guidelines, and implementation actions to continue the enhancement of HS and national security by protecting the United States and US interests from threats in the air domain. It directs multiple USG departments (including DOD) and

agencies to accomplish specific tasks that will improve the security and defense of the US homeland. Specifically, protection of critical transportation networks and infrastructure, enhancement of situational awareness, and enhancement of international relationships with allies and other partners.

(20) NSPD-23, *National Policy on Ballistic Missile Defense*. NSPD-23 acknowledges the various emerging threats to the United States – especially from WMD, and directs the SecDef to proceed with plans to deploy a set of initial missile defense capabilities.

(21) Presidential Decision Directive (PDD)-24, *US Counterintelligence Effectiveness*. PDD-24 is designed to foster increased cooperation, coordination and accountability among all US counterintelligence agencies. It directed the creation of a new national counterintelligence policy structure under the auspices of the NSC and directed the creation of a new National Counterintelligence Center. Nothing in this directive amends or changes the authorities and responsibilities of the SecDef.

(22) EO 13223, *Ordering the Ready Reserves of Armed Forces to Active Duty and Delegating Certain Authorities to the Secretary of Defense and the Secretary of Transportation*. Resulted from the September 14, 2001 Presidential Proclamation 7463: *Declaration of National Emergency by Reason of Certain Terrorist Attacks* and recognition of immediate threat of further attacks on the United States. It provides the DOD and DOT (now DHS) additional authorities, among them the ability to order any unit or member of the Ready Reserve to active duty and the transfer of select Title 10 USC provisions from the President to the respective department secretaries.

(23) EO 13231, *Critical Infrastructure Protection in the Information Age*. Designed to ensure the protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. Establishes national policy, scope of effort, and the President's Critical Infrastructure Protection Board. The order specifically identifies SecDef and Director of Central Intelligence with responsibility for National Security Information Systems.

(24) *Military Order of November 13, 2001, Federal Register: (Volume 66, Number 222)*. Military order from the President declaring a state of armed conflict exists since various terrorist attacks against the United States, which requires the use of the Armed Forces of the US. Acknowledges the use of the armed forces to identify terrorists and their supporters, to disrupt their activities, and to eliminate their ability to conduct or support terrorist attacks.

(25) EO 13292, *Further Amendment to Executive Order 12958, as Amended, Classified National Security Information*. Prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism.

(26) EO 13354, *National Counterterrorism Center*. Established the National Counterterrorism Center under the auspices of the Director of Central Intelligence. The center is intended to strengthen intelligence analysis and strategic planning and intelligence support to operations to counter transnational terrorist threats against the territory, people and interests of the United States. Support is intended for all agencies (includes DOD) consistent with applicable law.

(27) EO 13381, *Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information*. Addresses the protection of classified national security information against unauthorized disclosure and agency functions relating to determining eligibility for access to classified national security information.

(28) EO 13385, *Continuance of Certain Federal Advisory Committees and Amendments to and Revocation of Other Executive Orders*. Extended (until 30 September 2007) the existence of the National Infrastructure Advisory Council created by EO 13231.

(29) EO 13388, *Further Strengthening the Sharing of Terrorism Information to Protect American*. Further strengthens the effective conduct of US CT activities and is intended to protect the territory, people and interests of the United States, including against terrorist attacks.

(30) *The National Strategy for Homeland Security*. Prepared for the President by the Office of Homeland Security, this document lays out the strategic objectives, organization and critical areas for HS. The strategy identifies critical areas that focus on preventing terrorist attacks, reducing the nation's vulnerabilities, minimizing the damage and recovering from attacks that do occur. These critical areas are compatible with DOD's framework for HS that is discussed in this publication.

(31) *National Intelligence Strategy of the United States of America.* This document, among other objectives, has an enterprise objective to build an integrated intelligence capability to address threats to the homeland, consistent with US law and the protection of privacy and civil liberties. US intelligence elements must focus their capabilities to ensure that:

(a) Intelligence elements in the DOJ and HS are properly resourced and closely integrated within the larger IC.

(b) All IC components assist in facilitating the integration of collection and analysis against terrorists, WMD, and other threats to the homeland.

(c) State, local, and tribal entities and the private sector are connected to HS and intelligence efforts.

(32) *National Strategy for Combating Terrorism*. Expands on the NSHS and the NSS by expounding on the need to destroy terrorist organizations, win the war of ideas, and strengthen America's security at home and abroad. While the NSHS focuses on preventing

terrorist attacks within the United States, this strategy is more proactive and focuses on identifying and defusing threats before they reach our borders. The direct and continuous action against terrorist groups will disrupt, and over time, degrade and ultimately destroy their capability to attack the United States.

(33) *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Defines the road ahead for a core mission area identified in the President's NSHS – reducing the nation's vulnerability to acts of terrorism by protecting our critical infrastructures and key assets from physical attack. It identifies a clear set of national goals and objectives to achieve our protection goals. The strategy identifies thirteen critical infrastructure sectors. Key asset protection represents a broad array of unique facilities, sites, and structures whose disruption or destruction could have significant consequences across multiple dimensions. Examples include, but are not limited to nuclear power plants, national monuments, and commercial centers where large numbers of people congregate.

(34) *National Strategy to Secure Cyberspace*. An implementing component of the NSHS, it engages and empowers Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact. This will require a coordinated and focused effort from our entire society — the federal, state, and local governments. This strategy outlines a framework for organizing and prioritizing efforts, and calls upon individual Americans to improve our collective cyberspace security. It identifies three strategic objectives: prevent attacks in cyberspace against American critical infrastructure, reduce national vulnerability to attacks in cyberspace, and minimize damage and recovery time from attacks in cyberspace that do occur.

(35) *National Infrastructure Protection Plan*. The National Infrastructure Protection Plan provides a coordinated approach to critical infrastructure and key resource protection roles and responsibilities for federal, state, local, tribal, and private sector security partners. The National Infrastructure Protection Plan sets national priorities, goals, and requirements for effective distribution of funding and resources that will help ensure that our government, economy, and public services continue in the event of a terrorist attack or other disaster.

(36) *National Strategy for Maritime Security*. This document aligns all federal government maritime security programs and initiatives into a comprehensive and cohesive national effort involving appropriate federal, state, local, and private sector entities. There are eight supporting plans which when combined with the national strategy, presents a comprehensive national effort to promote global economic stability and protect legitimate activities while preventing hostile or illegal acts within the maritime domain. The document provides three broad principles as overarching guidance for maritime security:

(a) Outlines the President's vision for a fully coordinated USG effort to protect US interests in the maritime domain.

(b) Provides an overarching plan addressing all of the components of the maritime domain including domestic, international, public, and private components.

(c) Incorporates a global, cross-disciplined approach centered on a layered, defense-in-depth framework that may be adjusted on the threat level.

(d) This Strategy directs the coordination of the United States Government maritime security programs and initiatives to achieve a comprehensive national effort involving appropriate federal, state, tribal, local, and private sector entities. In support of this Strategy, eight national implementation plans provide amplifying detail and specificity:

1. National Plan to Achieve Maritime Domain Awareness lays the foundation for an effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of the United States, and identifying threats as early and as distant from our shores as possible.

2. Global Maritime Intelligence Integration Plan uses existing capabilities to integrate al available intelligence regarding potential threats to US interests in the maritime domain.

3. Maritime Operational Threat Response Plan aims for coordinated United States Government responses to threats against the United States and its interests in the maritime domain by establishing roles and responsibilities that enable the government to respond quickly and decisively.

4. International Outreach and Coordination Strategy provides a framework to coordinate all maritime security initiatives undertaken with foreign governments and international organizations, and solicits international support for enhanced maritime security.

5. Maritime Infrastructure Recovery Plan recommends procedures and standards for the recovery of the maritime infrastructure following attack or similar disruption.

6. Maritime Transportation System Security Plan responds to the President's call for recommendations to improve the national and international regulatory framework regarding the maritime domain.

7. Maritime Commerce Security Plan establishes a comprehensive plan to secure the maritime domain.

8. Domestic Outreach Plan engages non-Federal input to assist with the development and implementation of maritime security policies resulting from HSPD-13/NSPD-41.

(37) *National Security Strategy and the National Military Strategy*. The NSS establishes broad strategic guidance for advancing US interests in the global environment

through the instruments of national power. The NMS, derived from the NSS, focuses on how the Armed Forces of the United States will be employed to accomplish national strategic objective. The NSS and the NMS continue to reflect the first and fundamental commitment to defend the Nation against its adversaries.

(38) *National Southwest Border Counter Narcotics Strategy*. Addresses the land and air domains of the southwest border and the Mexican approaches and includes tasks for DOD. This Strategy affirms that the USG's counterdrug, counterterror, and immigration enforcement missions are interrelated and serves as an integrated component of the nation's efforts to secure the southwest border against all threats to the health and safety of the American people."

(39) *National Strategy for Aviation Security*. The strategy presents a vision for aviation security aimed at securing the people and interests of the United States. It underscores the Nation's commitment to strengthening international partnerships and advancing economic well-being around the globe by facilitating commerce and abiding by the principles of freedom of the airways.

(40) *Memorandum of Understanding Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing.* This agreement provides a framework and guidance to govern information sharing, use, and handling among the following individuals and their agencies: Secretary of Homeland Security, Director of Central Intelligence, the Attorney General, and any other organization having federal law enforcement responsibilities (other than those that are part of the DHS). The agreement mandates minimum requirements for information sharing, use, and handling and for coordination and deconfliction of analytic judgments.

(41) *National Military Strategic Plan For The War On Terrorism (NMSP-WOT)*. This constitutes the comprehensive military plan to prosecute the Global War on Terrorism for the Armed Forces of the United States. This document reflects the lessons of the first four years of the Global War on Terrorism, including the findings and recommendations of the 9-11 Commission and a rigorous examination within DOD, personally led by the SecDef and the CJCS. The NMSP-WOT outlines DOD's strategic planning and provides strategic guidance for military activities and operations in the Global War on Terrorism. The document guides the planning and actions of combatant commands, the military departments, combat support agencies and field support activities of the United States to protect and defend the homeland, attack terrorists and their capacity to operate effectively at home and abroad, and support mainstream efforts to reject violent extremism.

(42) **North American Aerospace Defense Agreement**. Agreement between the Government of the United States of America and the Government of Canada on the NORAD. Establishes the primary missions of NORAD that are: aerospace warning for North America; aerospace control for North America, and maritime warning for North America.

## 2. DOD Policy and Guidance

a. **Implications.** Specific authorities for HS missions are contained in federal and state law and policy documents. These form the basis for the development of DOD guidelines. These guidelines are promulgated in a variety of methods that include national strategy documents, planning guidance, and DODDs. These policy documents are consistent with and complementary to the federal statutes and guidelines discussed earlier in this appendix. DODDs specifically address HD mission.

b. **Key DOD Guidance.** The following discussion identifies a number of key documents to make commanders and planners more aware of material that may assist in the planning and execution of the HS mission areas.

(1) ***Strategy for Homeland Defense and Civil Support.*** Articulates strategic goals and objectives and provides direction to relevant HD activities across DOD. These activities include deterring and preventing attacks, protecting critical defense and designated civilian infrastructure, providing situational understanding, and preparing for and responding to incidents. The strategy focuses on building needed transformational capabilities, enhanced maritime awareness and response capability, strengthened allied contributions to collective security, and improved support to civil authorities.

(2) **Joint Planning Guidance** is part of the Planning, Programming, Budgeting and Execution Process to allocate resources within DOD. The Joint Planning Guidance is the link between planning and programming and it provides guidance to the DOD components for the development of their program proposal, known as the Program Objective Memorandum.

(3) **Contingency Planning Guidance (CPG)** provides guidance to the combatant commands concerning contingencies and includes the prioritized regional objectives for DOD. The CPG is a concise, classified document that SecDef uses to inform CJCS of general and specific strategic areas of concern to the civilian leadership for which contingency planning should be conducted. The Joint Staff collaborates with OSD in the initial drafting of the CPG. The final draft is coordinated with CJCS before it is forwarded to SecDef for his approval and subsequent submission to the NSC for presidential approval. After the CPG is published, the Joint Staff translates the policy guidance into specific planning guidance and tasks and inserts them into the Joint Strategic Capabilities Plan (JSCP).

(4) **Strategic Planning Guidance (SPG).** The SPG provides direction for DOD components to develop the Future Years Defense Program and the President's budget submission. The four defense policy goals are to assure, dissuade, deter, and decisively defeat. The goals are articulated in a planning construct of deterring forward and winning decisively while defending at home. The SPG additionally lists the priorities of SecDef: winning the Global War on Terrorism, strengthening our ability to meet our responsibilities, transforming the joint force, optimizing intelligence capabilities, counterproliferation, improving force manning, developing and implementing new concepts for global engagement, strengthening our ability to fulfill our responsibilities in HS, streamlining DOD

processes, and reorganizing DOD and the USG to deal with prewar opportunities and post-war responsibilities.

(5) **Strategic Military Intelligence Review** establishes core intelligence issues of highest priority, identifies needs and gaps, and provides a common framework and substantive guidance for allocating intelligence collection and production resources.

(6) **Joint Strategy Review (JSR).** The JSR helps the Joint Staff integrate strategy, operational planning, and program assessments. It covers the short, mid and long-term periods: 0-2, 2-10, and 10-20 years in the future. The JSR assesses the global strategic setting for issues affecting the NMS.

(7) **Unified Command Plan.** The UCP provides basic guidance to all unified CCDRs; establishes their missions, responsibilities, and force structure; delineates the general geographical AORs for geographic CCDRs; and specifies functional responsibilities for functional CCDRs.

(8) **Security Cooperation Guidance (SCG).** Security cooperation is the means by which DOD encourages and enables countries and organizations to work with us to achieve strategic objectives. The SCG provides the foundation for all DOD interactions with foreign defense establishments and supports the President's National Security Strategy. It describes the SecDef's priorities for creating new partnerships and building the capacity of existing partnerships."

(9) **DODD 2000.12, *DOD Antiterrorism Program*.** This directive updates policies and assigns responsibilities for implementing the procedures for DOD's AT program. It establishes CJCS as the principal advisor and focal point responsible to SecDef for DOD AT issues. It also defines the AT responsibilities of the Military Departments, combatant commands, DOD agencies, and DOD field activities. Its guidelines are applicable for the physical security of all DOD activities both overseas and in the homeland.

(10) **DODD 3000.05, *Military Support for Stability, Security, Transition, and Reconstruction (SSTR) Operations.*** This directive provides guidance on stability operations that will evolve over time as joint operating concepts, mission sets, and lessons learned develop. It establishes DOD policy and assigns responsibilities within DOD for planning, training, and preparing to conduct and support stability operations pursuant to the authority vested in SecDef under Sections 113 and 153 of Title 10, USC, and the guidance and responsibilities assigned in the SPG for Fiscal Year 2006-2011.

(11) **DODD 3020.40, *Defense Critical Infrastructure Program***. This directive establishes policy and assigns responsibilities for DCI activities as they apply to DOD, and authorizes ASD (HD&ASA) to issue instructions and guidance for the implementation of this directive.

(12) **DODD 4630.5, *Interoperability and Supportability of Information Technology and National Security Systems*** defines a capability-focused, effects-based

approach to advance information technology and national security systems interoperability and supportability across DOD.

(13) **DODD 5100.78,** ***United States Port Security Program*** outlines the authorities, responsibilities, and functions relative to appropriate security measures and programs to counter the threat posed to US ports.

(14) **DODD 5200.27,** ***Acquisition of Information Concerning Persons and Organizations not Affiliated with DOD***. This directive establishes the Defense Investigative Program general policy, limitations, procedures, and operational guidance pertaining to the collecting, processing, storing, and disseminating of information concerning persons and organizations not affiliated with DOD.

(15) **DODD 5205.5,** ***DOD Operations Security (OPSEC) Program*** provides policy and responsibilities governing DOD's OPSEC program and incorporates the requirements of National Security Decision Directive, 298 that apply to DOD. It underscores the importance of OPSEC and how it is integrated as a core military capability within IO that must be followed in daily application of military operations.

(16) **DODD 5240.1,** ***DOD Intelligence Activities*** provides guidance to DOD intelligence components to collect, retain, or disseminate information concerning US persons.

(17) **CJCSI 3100.01A,** ***Joint Strategic Planning System*** provides joint policy and guidance on, and describes the responsibilities and functions of, the joint strategic planning system. Provides expanded guidance on the process for developing combatant command theater engagement plans and identifies the plan approval process.

(18) **CJSCI 3121.01B,** ***Standing Rules of Engagement and Standing Rules for the Use of Force for US Forces (U).*** This instruction establishes rules regarding the use of force by DOD personnel during military operations.

(19) **CJSCI 3213.01B,** ***Joint Operations Security.*** Provides policy and guidance for planning and executing OPSEC in support of joint military operations.

(20) **CJSCI 3610.01A,** ***Aircraft Piracy (Hijacking) and Destruction of Derelict Airborne Objects*** provides guidance to the Deputy Director for Operations, National Military Command Center, and operational commanders in the event of an aircraft piracy (hijacking) or request for destruction of derelict airborne objects.

(21) **CJCSI 3710.01A,** ***DOD Counterdrug Operational Support***. This instruction promulgates SecDef delegation of authority to approve certain CD operational support missions. It also provides, in accordance with the Fiscal Year 1991 National Defense Authorization Act, as amended, instruction on authorized types of DOD (Title 10 USC) CD support to the federal agency with lead responsibility, other government agencies, and foreign nations.

(22) **CJCSI 5221.01B,** ***Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations.*** This instruction explains the authority delegated by CJCS to the CCDRs concerning the disclosure of classified military information for which they are the originating component to foreign governments and international organizations.

(23) **CJCSI 5810.01B,** ***Implementation of the DOD Law of War Program*** establishes joint policy, assigns responsibilities, and provides guidance regarding the US law of war obligations. It also assigns specific responsibilities within DOD to ensure compliance with the law of war.

(24) ***Memorandum of Agreement Between the Department of Defense and Department of Homeland Security for Department of Defense Support to the United States Coast Guard for Maritime Homeland Security.*** Identifies and documents appropriate capabilities, roles, missions and functions for DOD in support of the USCG when conducting maritime HS operations, and to facilitate the rapid flow of DOD forces to the USCG in support of maritime HS operations.

(25) ***Memorandum of Agreement between Department of Defense and Department of Homeland Security for the Inclusion of the US Coast Guard in support of Maritime Homeland Defense***. Establishes DOD joint C2 structure for maritime HD operations that include USCG forces and to identifies and documents appropriate roles, missions, and functions for the USCG in support of maritime HD operations.

# APPENDIX E
# REFERENCES

The development of JP 3-27 is based on the following primary references:

## 1. General

a. US Constitution.

b. EO 12333, *United States Intelligence Activities*.

c. EO 12656, *Assignment of Emergency Preparedness Responsibilities*.

d. EO 13228, *Establishing the Office of Homeland Security and the Homeland Security Council*.

e. EO 13231, *Critical Infrastructure Protection in the Information Age*.

f. EO 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans*.

g. EO 13223, *Ordering the Ready Reserves of Armed Forces to Active Duty and Delegating Certain Authorities to the Secretary of Defense and the Secretary of Transportation*.

h. *Military Order of* 13 November 2001.

i. EO 13293, *Further Amendment to Executive Order 12958, as Amended*, *Classified National Security Information*.

j. EO 13316, *Continuance of Certain Federal Advisory Committees*.

k. EO 13354, *National Counterterrorism Center*.

l. EO 13381, *Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information*.

m. EO 13385, *Further Strengthening the Sharing of Terrorism Information to Protect American*.

n. *National Response Plan*.

o. NSPD-1, *Organization of the National Security Council System.*

p. HSPD-1, *Organization and Operations of the Homeland Security Council*.

q. HSPD-2, *Combating Terrorism Through Immigration Policies*.

r. HSPD-3, *Homeland Security Advisory System*.

s. HSPD-4/NSPD-17, *National Strategy to Combat Weapons of Mass Destruction*.

t. HSPD-5, *Management of Domestic Incidents*.

u. HSPD-6, *Integration and Use of Screening Information*.

v. HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*.

w. HSPD-8, *National Preparedness*.

x. HSPD-10/NSPD-33, *Biodefense for the 21st Century*.

y. HSPD-11, *Comprehensive Terrorist-Related Screening Procedures*.

z. HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*.

aa. HSPD-13/NSPD-41, *Maritime Security Policy*.

ab. HSPD-14/NSPD-43, *Domestic Nuclear Detection Office*.

ac. HSPD-15/NSPD-46, *US Strategy and Policy in the War on Terror.*

ad. HSPD-16/NSPD-47, *US Aviation Security Policy.*

ae. National Military Strategy.

af. NSPD-23, *National Policy on Ballistic Missile Defense*.

ag. NSPD-33, *Biodefense for the 21st Century*.

ah. National Security Strategy.

ai. National Strategy for Homeland Security.

aj. National Strategy for Physical Protection of Critical Infrastructure and Key Assets.

ak. National Strategy for Combating Terrorism.

al. National Strategy to Secure Cyberspace.

am. National Strategy for Maritime Security.

an. National Intelligence Strategy of the United States of America.

ao. Maritime Strategy for Homeland Security.

ap. Maritime Operational Threat Response Plan.

aq. National Industrial Security Program.

ar. The North American Aerospace Defense Command (NORAD) Agreement and Terms of Reference.

as. Canada-US Rush-Baggot Treaty.

at. CANUS Basic Security Document 100/35.

au. NORAD Instruction 10-24.

av. Operation NOBLE EAGLE (ONE) Tactics, Techniques and Procedures Reference Guide.

aw. PDD-14, *Counternarcotics*.

ax. PDD-24, *US Counterintelligence*.

ay. PDD-67, *Enduring Constitutional Government and Continuity of Government Operations.*

az. Title 10, USC, *Armed Forces*.

ba. Title 14, USC, *United States Coast Guard*.

bb. Title 18, USC, Section 1385, *The Posse Comitatus Act*.

bc. Title 32, USC, *National Guard*.

bd. Title 33, USC, *Navigation and Navigable Waters.*

be. Title 42 USC Section 9601, "*Comprehensive Environmental Response, Compensation, and Liability Act.*

bf. Title 46, USC, *Shipping.*

bg. Title 50, USC, *War and National Defense.*

bh. The Homeland Security Act of 2002.

bi. UFC 4-010-01, *DOD Minimum Standards for Buildings.*

bj. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act).

bk. The National Defense Authorization Act of 2002.

bl. Unified Command Plan.

bm. United States Government Interagency Domestic Terrorism Concept of Operations Plan.

bn. US Department of Homeland Security, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in the New World*.

bo. Memorandum of Understanding Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing.

### 2. Department of Defense Documents

a. SecDef Memorandum, Forces for Unified Commands.

b. DODD 2000.12, *DOD Antiterrorism (AT) Program*.

c. DODD 1300.17, *Accommodation of Religious Practices Within the Military Services*.

d. DODD 3000.05, *Military Support for Stability, Security, Transition, and Reconstruction (SSTR) Operations*.

e. DODD 3020, *Defense Critical Infrastructure Program*.

f. DODD 3020.26, *Defense Continuity Program*.

g. DODD 3020.36, *Assignment of National Security EP(NSEP) Responsibilities to DOD Components*.

h. DODD 3020.40, *Defense Critical Infrastructure Identification, Prioritization, and Protection Defense Critical Infrastructure Program*.

i. DODD 4630.5, *Interoperability and Supportability of Information Technology and National Security Systems*.

j. DODD 5100.1, *Functions of the DOD and Its Major Components*.

k. DODD 5105.19, *Defense Information Systems Agency (DISA)*.

l. DODD 5100.78, *United States Port Security Program*.

m. DODD 5148.11, *Assistant to the Secretary of Defense for Intelligence Oversight (ATSD IO)*.

n. DODD 5200.27, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the DOD*.

o. DODD 5205.5, *DOD Operations Security (OPSEC) Program*.

p. DODD 5210.56, *Use of Deadly Force and the Carrying of Firearms by DOD Personnel in Law Enforcement and Security Duties*.

q. DODD 5220.22, *National Industrial Security Program*.

r. DODD 5240.1, *DOD Intelligence Activities*.

s. DODD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons*.

t. DODD 5525.5, *DOD Cooperation with Civilian Law Enforcement Officials*.

u. DODI 3020, *Implementation of the Critical Infrastructure Program.*

v. DODI 2000.16, *DOD Antiterrorism Standards*.

w. Joint Planning Guidance.

x. Strategic Planning Guidance.

y. Contingency Planning Guidance.

z. National Geospatial Intelligence Agency Geospatial Intelligence Series (GIPS).

aa. National Infrastructure Protection Plan.

ab. Joint Strategic Capabilities Plan.

ac. Memorandum of Agreement Between the Department of Defense and the Department of Homeland Security for Inclusion of the US Coast Guard in Support of Maritime Homeland Defense.

ad. Memorandum of Agreement Between the Department of Defense and the Department of Homeland Security for Department of Defense Support to the United States Coast Guard for Maritime Homeland Security.

ae. Global Force Management Guidance" Section II, Assignment of Forces (Forces For Unified Commands).

af. National Defense Strategy of the United States of America.

ag. National Military Strategy for Cyberspace Operations.

ah. Strategic Planning Guidance.

ai. Strategy for Homeland Defense and Civil Support.

### 3. Joint Publications

a. JP 1, *Doctrine for the Armed Forces of the United States*.

b. JP 1-0, *Personnel Support to Joint Operations.*

c. JP 1-02, *DOD Dictionary of Military and Associated Terms*.

d. JP 1-05, *Religious Support for Joint Operations*.

e. JP 2-0, *Joint Intelligence*.

f. JP 2-01. *Joint and National Intelligence Support to Military Operations*.

g. JP 3-0, *Joint Operations*.

h. JP 3-01, *Countering Air and Missile Threats*.

i. JP 3-03, *Joint Interdiction Operations.*

j. JP 3-07.2, *Antiterrorism*.

k. JP 3-07.4, *Joint Counterdrug Operations*.

l. JP 3-08 (Vols I & II), *Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations*.

m. JP 3-09.3, *Joint Tactics, Techniques, and Procedures for Close Air Support (CAS).*

n. JP 3-11, *Joint Doctrine for Operations in Nuclear, Biological, and Chemical (NBC) Environments*.

o. JP 3-13, *Information Operations.*

p. JP 3-13.3, *Operations Security*.

q. JP 3-14, *Joint Doctrine for Space Operations*.

r. JP 3-16, *Multinational Operations.*

s. JP 3-28, *Civil Support.*

t. JP 3-30, *Command and Control for Joint Air Operations*.

u. JP 3-31, *Command and Control for Joint Land Operations*.

v. JP 3-32, *Command and Control for Joint Maritime Operations*.

w. JP 3-33, *Joint Task Force Headquarters*.

x. JP 3-34, *Joint Engineer Operations*.

y. JP 3-35, *Joint Deployment and Redeployment Operations.*

z. JP 3-40, *Joint Doctrine for Combating Weapons of Mass Destruction*.

aa. JP 3-41, *Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives Consequence Management*.

ab. JP 3-52, *Joint Doctrine for Airspace Control in the Combat Zone*.

ac. JP 3-53, *Doctrine for Joint Psychological Operations*.

ad. JP 3-60, *Joint Targeting.*

ae. JP 3-61, *Public Affairs*.

af. JP 4-0, *Logistic Support of Joint Operations*.

ag. JP 4-02, *Health Service Support*.

ah. JP 4-05.1, *Joint Manpower Mobilization and Demobilization Operations: Reserve Component Call-up.*

ai. JP4-06, *Mortuary Affairs in Joint Operations*.

aj. JP 5-0, *Joint Operation Planning*.

ak. JP 6-0*, Joint Communications System.*

al. Domestic Operational Law (DOPLAW) Handbook for Judge Advocates.

am. Maritime Law Enforcement Manual.

an. CJCSI 1301.01C, *Individual Augmentation Procedures*.

ao. CJCSI 3110.01, *Joint Strategic Capabilities Plan FY 2002 (U).*

ap. CJCSI 3100.01A, *Joint Strategic Planning System*.

aq. CJCSI 3121.01B, *Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces (U).*

ar. CJCSI 3213.01B, *Joint Operations Security*.

as. CJCSI 3610.01A, *Aircraft Piracy (Hijacking) and Destruction of Derelict Airborne Objects*.

at. CJCSI 3710.01A, *DOD Counterdrug Support*.

au. CJCSI 4120.02, *Assignment of Movement Priority*.

av. CJCSI 5113.02A, *Chairman of the Joint Chiefs of Staff Counterproliferation Charter (U)*.

aw. CJCSI 5120.02A, *Joint Doctrine Development System*.

ax. CJCSI 5221.01B, *Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations*.

ay. CJCSI 5810.01B, *Implementation of the DOD Law of War Program*.

### 4. Multi-Service Publications

a. FM 3-22.40 / NTTP 3-07.3.2 / MCWP 3-15.8 / AFTTP 3-2.45 / USCG Pub 3-07.31, *NLW – Tactical Employment of Non Lethal Weapons.*

b. FM 3-01.1 / NTTP 3-26.1.1 / AFTTP) 3-2.50, *ADUS -- Air Defense of the United States (U).*

c. NTTP 3-07.11 / CGP 3-07.11, *Maritime Interception Operations.*

### 5. Army Publications

a. FM 1, *The Army*.

b. FM 3-0, *Operations*.

### 6. Navy Publications

a. Naval Doctrine Publication 1, *Naval Warfare*.

b. Naval Warfare Publication 3-10, *Naval Coastal Warfare*.

### 7. Marine Corps Publications

Marine Corps Doctrinal Publication 1, *Warfighting,* 6 March 1989.

### 8. Air Force Publications

a. Air Force Doctrine Document (AFDD) 1, *Air Force Basic Doctrine*.

b. AFDD 2-10, *Homeland Operations*.

c. AFDD 2-4.2, *Health Services*.

d. Air Force Instruction 10-2701, *Organization and Function of the Civil Air Patrol*.

### 9. Coast Guard Publications

a. Coast Guard Publication-1, *US Coast Guard: America's Maritime Guardian*.

b. Coast Guard Publication 3-01, *Maritime Strategy for Homeland Security*.

### 10. USNORTHCOM Publications

a. USNORTHCOM Concept of Operations.

b. USNORTHCOM Homeland Defense Concept of Employment.

c. USNORTHCOM-NGB Joint Continental United States (CONUS) Communications Support Environment (JCCSE) Concept.

d. USNORTHCOM Antiterrorism (AT) Operations Order.

Intentionally Blank

# APPENDIX F
# ADMINISTRATIVE INSTRUCTIONS

## 1. User Comments

Users in the field are highly encouraged to submit comments on this publication to: Commander, United States Joint Forces Command, Joint Warfighting Center ATTN: Doctrine and Education Group, 116 Lake View Parkway, Suffolk, VA 23435-2697. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

## 2. Authorship

The lead agent for this publication is CDRUSNORTHCOM. The Joint Staff doctrine sponsor for this publication is the Director for Operations (J-3).

## 3. Supersession

This publication supersedes JP 3-01.1, 04 November 1996, *Aerospace Defense of North America*. This publication, in conjunction with the publication of JP 3-28, 14 September 2007, *Civil Support*, supersedes JP 3-26, 02 August 2005, *Homeland Security*.

## 4. Change Recommendations

a. Recommendations for urgent changes to this publication should be submitted:

TO: CDR NORTHCOM
INFO: JOINT STAFF WASHINGTON DC//J7-JEDD//
CDR USJFCOM SUFFOLK VA//DOCGP//

Routine changes should be submitted electronically to Commander, Joint Warfighting Center, Doctrine and Education Group and info to the lead agent and the Director for Operational Plans and Joint Force Development (J-7), JEDD.

b. When a Joint Staff directorate submits a proposal to the Chairman of the Joint Chiefs of Staff that would change source document information reflected in this publication, that directorate will include a proposed change to this publication as an enclosure to its proposal. The Military Services and other organizations are requested to notify the Director, J-7, Joint Staff, when changes to source documents reflected in this publication are initiated.

c. Record of Changes:

| CHANGE NUMBER | COPY NUMBER | DATE OF CHANGE | DATE ENTERED | POSTED BY | REMARKS |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

## 5. Distribution of Publications

a. Local reproduction is authorized and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified joint publications must be in accordance with DOD Regulation 5200.1 R, *Information Security Program*.

## 6. Distribution of Electronic Publications

a. Joint Staff J-7 will not print copies of JPs for distribution. Electronic versions are available on JDEIS at https://jdeis.js.mil (NIPRNET), and https://jdeis.js.smil.mil (SIPRNET) and on the JEL at http://www.dtic.mil/doctrine (NIPRNET).

b. Only approved joint publications and joint test publications are releasable outside the combatant commands, Services, and Joint Staff. Release of any classified joint publication to foreign governments or foreign nationals must be requested through the local embassy (Defense Attaché Office) to DIA Foreign Liaison Office, PO-FL, Room 1E811, 7400 Pentagon, Washington, DC 20301-7400.

c. CD-ROM. Upon request of a JDDC member, the Joint Staff J-7 will produce and deliver one CD-ROM with current joint publications.

# GLOSSARY
## PART I — ABBREVIATIONS AND ACRONYMS

| | |
|---|---|
| AC | Active Component |
| ACC | Air Combat Command |
| ADS | air defense sector |
| AFB | Air Force base |
| AFDD | Air Force doctrine document |
| AFNORTH | Air Forces Northern |
| AFTTP | Air Force tactics techniques, and procedures |
| ALCOM | US Alaskan Command |
| ANG | Air National Guard |
| ANGUS | Air National Guard of the United States |
| ANR | Alaskan North American Aerospace Defense Command Region |
| AO | area of operations |
| AOR | area of responsibility |
| AOTR | Aviation Operational Threat Response |
| ARNG | Army National Guard |
| ARNGUS | Army National Guard of the United States |
| ASBPO | Armed Services Blood Program Office |
| ASD(HA) | Assistant Secretary of Defense (Health Affairs) |
| ASD(HD&ASA) | Assistant Secretary of Defense (Homeland Defense and America's Security Affairs) |
| ASD(NII) | Assistant Secretary of Defense (Networks and Information Integration) |
| ASD(RA) | Assistant Secretary of Defense (Reserve Affairs) |
| ASD(SO/LIC&IC) | Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict and Interdependent Capabilities) |
| AT | antiterrorism |
| ATSD(NCB) | Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs |
| BI | battlefield injury |
| BMD | ballistic missile defense |
| BSI | base support installation |
| C2 | command and control |
| CAA | command arrangement agreement |
| CAD | Canadian air division |
| CANADA COM | Canada Command |
| CANR | Canadian North American Aerospace Defense Command Region |
| CANUS | Canada-United States |
| CAP | Civil Air Patrol |
| CBRNE | chemical, biological, radiological, nuclear, or high-yield explosives |
| CCDR | combatant commander |
| CD | counterdrug |
| CDR | commander |
| CDRNORAD | Commander, North American Aerospace Defense Command |

| | |
|---|---|
| CDRUSARNORTH | Commander, US Army North |
| CDRUSCENTCOM | Commander, United States Central Command |
| CDRUSELEMNORAD | Commander, United States Element, North American Aerospace Defense Command |
| CDRUSEUCOM | Commander, United States European Command |
| CDRUSJFCOM | Commander, United States Joint Forces Command |
| CDRUSNORTHCOM | Commander, United States Northern Command |
| CDRUSPACOM | Commander, United States Pacific Command |
| CDRUSSOCOM | Commander, United States Special Operations Command |
| CDRUSSOUTHCOM | Commander, United States Southern Command |
| CDRUSSTRATCOM | Commander, United States Strategic Command |
| CDRUSTRANSCOM | Commander, United States Transportation Command |
| CDS | Canadian Chief of Defence Staff |
| CFB | Canadian forces base |
| CG | commanding general |
| CGDEFOR | Coast Guard defense force |
| CIA | Central Intelligence Agency |
| CIO | chief information officer |
| CIP | critical infrastructure protection |
| CJCS | Chairman of the Joint Chiefs of Staff |
| CJCSI | Chairman of the Joint Chiefs of Staff instruction |
| CJTF | commander, joint task force |
| CM | consequence management |
| CNGB | Chief, National Guard Bureau |
| COCOM | combatant command (command authority) |
| COG | continuity of government |
| COM | command |
| COMMARFORNORTH | Commander, Marine Corps Forces North |
| COMPACAF | Commander, Pacific Air Forces |
| COMPACFLT | Commander, Pacific Fleet |
| COMUSFLTFORSCOM | Commander, US Fleet Forces Command |
| CONPLAN | concept plan |
| CONR | Continental United States North American Aerospace Defense Command Region |
| CONUS | continental United States |
| COOP | continuity of operations |
| COP | common operational picture |
| COTP | captain of the port |
| CPG | Contingency Planning Guidance |
| CrM | crisis management |
| CS | civil support |
| CSA | combat support agency |
| CSS | combat service support |
| CT | counterterrorism |
| | |
| DAFL | directive authority for logistics |

| | |
|---|---|
| DCI | defense critical infrastructure |
| DCIP | Defense Critical Infrastructure Program |
| DCMA | Defense Contract Management Agency |
| DCST | Defense Logistics Agency (DLA) contingency support team |
| DEST | domestic emergency support team |
| DHHS | Department of Health and Human Services |
| DHS | Department of Homeland Security |
| DIA | Defense Intelligence Agency |
| DIB | defense industrial base |
| DISA | Defense Information Systems Agency |
| DLA | Defense Logistics Agency |
| DNBI | disease and nonbattle injury |
| DNDO | Domestic Nuclear Detection Office |
| DOD | Department of Defense |
| DODD | Department of Defense directive |
| DODI | Department of Defense instruction |
| DOE | Department of Energy |
| DOJ | Department of Justice |
| DOT | Department of Transportation |
| DSA | defensive sea area |
| DTIP | Disruptive Technology Innovations Partnership |
| DTRA | Defense Threat Reduction Agency |
| | |
| EADS | Eastern Air Defense Sector |
| EMIO | expanded maritime interception operations |
| EO | executive order |
| EP | emergency preparedness |
| EPA | Environmental Protection Agency |
| EXORD | execute order |
| | |
| FAA | Federal Aviation Administration |
| FBI | Federal Bureau of Investigation |
| FEMA | Federal Emergency Management Agency |
| FHP | force health protection |
| FM | field manual (Army) |
| FP | force protection |
| | |
| GCC | geographic combatant commander |
| GEOINT | geospatial intelligence |
| GIG | Global Information Grid |
| GPS | global positioning system |
| GSA | General Services Administration |

| | |
|---|---|
| HD | homeland defense |
| HDC | harbor defense commander |
| HHS | Department of Health and Human Services |
| HS | homeland security |
| HSAC | Homeland Security Advisory Council |
| HSC | Homeland Security Council |
| HSPD | homeland security Presidential directive |
| HVA | high value asset |
| | |
| IA | information assurance |
| IACG | interagency coordination group |
| IAW | in accordance with |
| IC | intelligence community |
| IFP | integrated force package |
| IGO | intergovernmental organization |
| IMPT | incident management planning team |
| IO | information operations |
| IPC | interagency planning cell |
| ISG | information synchronization group |
| ISR | intelligence, surveillance, and reconnaissance |
| ITW/AA | integrated tactical warning/and attack assessment |
| | |
| J-1 | manpower and personnel directorate of a joint staff |
| J-2 | intelligence directorate of a joint staff |
| J-3 | operations directorate of a joint staff |
| J-4 | logistics directorate of a joint staff |
| J-6 | communications system directorate of a joint staff |
| J-A | judge advocate directorate of a joint staff |
| JFACC | joint force air component commander |
| JFC | joint force commander |
| JFCC-IMD | Joint Functional Component Command for Integrated Missile Defense |
| JFCC-ISR | joint Functional Component Command for Intelligence, Surveillance, And Reconnaissance |
| JFHQ | joint force headquarters |
| JFHQ-NCR | Joint Force Headquarters-National Capital Region |
| JFLCC | joint force land component commander |
| JFMCC | joint force maritime component commander |
| JIACG | joint interagency coordination group |
| JOA | joint operations area |
| JOC | joint operations center |
| JP | joint publication |
| JRSOI | joint reception, staging, onward movement, and integration |
| JSCP | Joint Strategic Capabilities Plan |
| JSR | Joint Strategic Review |
| JTF | joint task force |

| | |
|---|---|
| JTF-AK | Joint Task Force-Alaska |
| JTF-CS | Joint Task Force – Civil Support |
| JTF-GNO | Joint task Force-Global Network Operations |
| JTF-HD | Joint Task Force-Homeland Defense |
| JTF-N | Joint Task Force-North |
| | |
| LEA | law enforcement agency |
| LNO | liaison officer |
| | |
| MARFORNORTH | Marine Corps Forces, North |
| MARFORSOUTH | Marine Corps Forces South |
| MCM | mine countermeasures |
| MCWP | Marine Corps warfighting publication |
| MIO | maritime interception operations |
| MOA | memorandum of agreement |
| MOTR | maritime operational threat response |
| MOU | memorandum of understanding |
| | |
| NAVFAC | Naval Facilities Engineering Command |
| NCC | National Coordinating Center |
| NCR | National Capital Region (US) |
| NCRCC | National Capital Region Coordination Center |
| NCRCG | National Cyber response Coordination Group |
| NCR-IADS | National Capital Region – Integrated Air Defense System |
| NCS | National Communications System |
| NDHQ | Department of National Defence |
| NDDOC | US Northern Command Deployment and Distribution Operations Center |
| NETOPS | network operations |
| NG | National Guard |
| NGA | National Geospatial-Intelligence Agency |
| NGB | National Guard Bureau |
| NGO | nongovernmental organization |
| NIPRNET | Non-Secure Internet Protocol Router Network |
| NIRT | Nuclear Incident Response Team |
| NLW | nonlethal weapon |
| NMS | national military strategy |
| NMS-CO | National Military Strategy for Cyberspace Operations |
| NOC | National Operations Center |
| NORAD | North American Aerospace Defense Command |
| NRP | National Response Plan |
| NSA | National Security Agency |
| NSC | National Security Council |
| NSHS | National Strategy for Homeland Security |
| NSMS | National Strategy for Maritime Security |
| NSPD | national security Presidential directive |

| | |
|---|---|
| NSS | National Security Strategy |
| NST | National Geospatial-Intelligence Agency support team |
| NTTP | Navy tactics, techniques, and procedures |
| NVDT | National Geospatial-Intelligence Agency voluntary deployment team |
| OCA | offensive counterair |
| OEH | occupational and environmental health |
| OI&A | Office of Intelligence and Analysis (DHS) |
| ONE | Operation NOBLE EAGLE |
| OPCON | operational control |
| OPLAN | operation plan |
| OPSEC | operations security |
| OSD | Office of the Secretary of Defense |
| PA | public affairs |
| PCA | Posse Comitatus Act |
| PCC | policy coordination committee |
| PDD | Presidential decision directive |
| POD | port of debarkation |
| PRC | Presidential Reserve Call-up |
| PS/HD | port security/harbor defense |
| PSI | Proliferation Security Initiative |
| PSYOP | psychological operations |
| QRF | quick response force |
| RC | Reserve Component |
| ROE | rules of engagement |
| RFF | request for forces |
| RRF | rapid response force |
| RS | religious support |
| RST | religious support team |
| RUF | rules for the use of force |
| S&T | science and technology |
| SAOC | sector air operations center |
| SATCOM | satellite communications |
| SCG | Security Cooperation Guidance |
| SCP | security cooperation plan |
| SecDef | Secretary of Defense |
| SIGINT | signals intelligence |
| SIPRNET | SECRET Internet Protocol Router Network |
| SJFHQ-North | Standing Joint Force Headquarters - North |
| SO | special operations |
| SOCPAC | Special Operations Command Pacific |

| | |
|---|---|
| SOF | special operations forces |
| SPG | Strategic Planning Guidance |
| SPOE | seaport of embarkation |
| SROE | standing rules of engagement |
| SRUF | standing rules for the use of force |
| | |
| TAA | tactical assembly area |
| TACON | tactical control |
| TNCC | theater network operations (NETOPS) control center |
| TPMRC | theater patient movement requirements center |
| TSA | Transportation Security Administration |
| | |
| UCP | Unified Command Plan |
| UFC | Unified Facilities Criteria |
| USACE | US Army Corps of Engineers |
| USAFR | United States Air Force Reserve |
| USAR | United States Army Reserve |
| USARNORTH | US Army Forces North |
| USARPAC | United States Army Pacific Command |
| USARSO | United States Army Southern Command |
| USC | United States Code |
| USCG | United States Coast Guard |
| USCGR | United States Coast Guard Reserve |
| USDA | United States Department of Agriculture |
| USD(P) | Under Secretary of Defense for Policy |
| USELEMNORAD | United States Element North American Aerospace Defense Command |
| USEUCOM | United States European Command |
| USG | United States Government |
| USJFCOM | United States Joint Forces Command |
| USMCR | United States Marine Corps Reserve |
| USN | United States Navy |
| USNAVSO | US Naval Forces Southern Command |
| USNORTHCOM | United States Northern Command |
| USNR | United States Navy Reserve |
| USPACOM | United States Pacific Command |
| USSOCOM | United States Special Operations Command |
| USSOUTHCOM | United States Southern Command |
| USSTRATCOM | United States Strategic Command |
| USTRANSCOM | United States Transportation Command |
| | |
| WADS | Western Air Defense Sector |
| WMD | weapons of mass destruction |

## PART II — TERMS AND DEFINITIONS

Unless otherwise annotated, this publication is the proponent for all terms and definitions found in the glossary. JP 1-02 will reflect this publication as the source document for these terms and definitions.

**base support installation**. A Department of Defense service or agency installation within the United States, its territories, or possessions tasked to serve as a base for military forces engaged in either homeland defense or civil support operations. Provides general support logistics and administrative support to military forces. Also called BSI. (This term and its definition are provided for information and are proposed for inclusion in JP 1-02 by JP 3-28.)

**defense critical infrastructure.** Department of Defense and non-Department of Defense networked assets and essential to project, support, and sustain military forces and operations worldwide. Also called DCI. (JP 1-02)

**domestic emergencies.** Emergencies affecting the public welfare and occurring within the 50 states, District of Columbia, Commonwealth of Puerto Rico, US possessions and territories, or any political subdivision thereof, as a result of enemy attack, insurrection, civil disturbance, earthquake, fire, flood, or other public disasters or equivalent emergencies that endanger life and property or disrupt the usual process of government. Domestic emergencies include civil defense emergencies, civil disturbances, major disasters, and natural disasters. (This term and its definition modify the existing term and its definition and are approved for inclusion in JP 1-02.)

**global strike.** A rapidly planned, limited-duration, extended-range precision attack that is conducted to achieve strategic objectives. (This term and its definition are applicable only in the context of this publication and cannot be referenced outside this publication.)

**homeland.** The physical region that includes the continental United States, Alaska, Hawaii, United States territories and possessions, and surrounding territorial waters and airspace. (JP 1-02)

**homeland defense.** The protection of United States sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression or other threats as directed by the President. Also called HD. (This term and its definition modify the existing term and its definition and are approved for inclusion in JP 1-02.)

**homeland security.** As defined in the National Strategy for Homeland Security, a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. The Department of Defense contributes to homeland security through its military missions overseas, homeland defense, and support to civil authorities. Also called HS. (This term and its definition modify the existing term and its definition and are approved for inclusion in JP 1-02.)

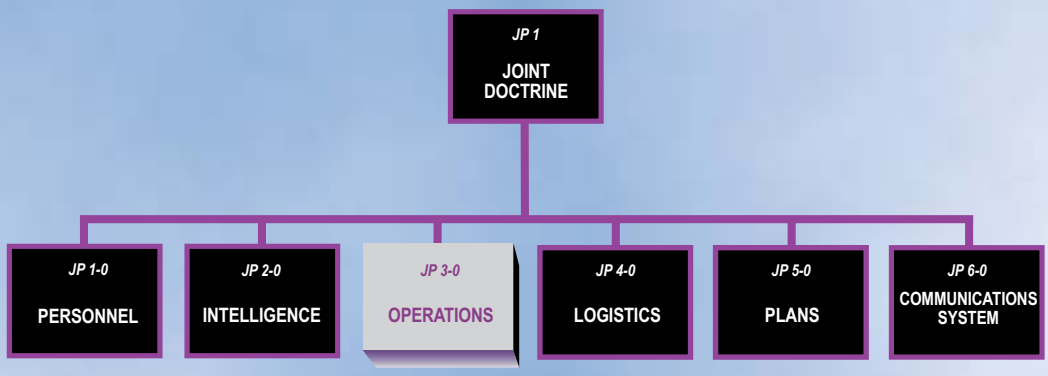
**primary agency.** The federal department or agency assigned primary responsibility for managing and coordinating a specific emergency support function in the National Response Plan. (This term and its definition are provided for information and proposed for inclusion in JP 1-02 by JP 3-28.)

**quick response force.** A company-sized force providing responsive, mission-tailored, lightly armed ground units that can deploy on short notice, with minimal lift assets, and capable of providing immediate or emergency response. Also called QRF. (Approved for inclusion in JP 1-02.)

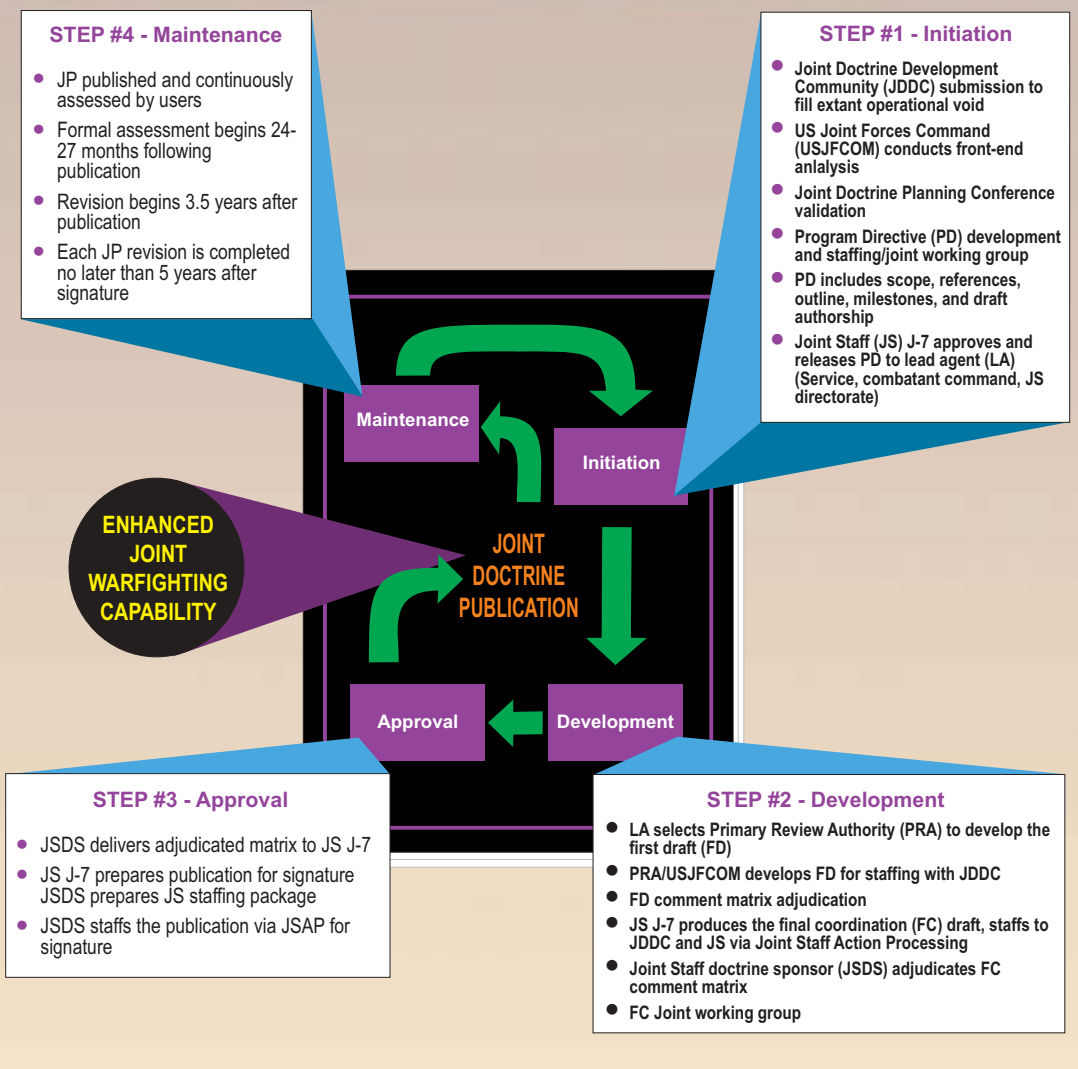
**rapid response force.** A battalion minus-sized force providing responsive, mission-tailored, lightly armed ground units that can deploy on short notice, with minimal lift assets, and capable of providing immediate or emergency response. Also called RRF. (Approved for inclusion in JP 1-02.)

Intentionally Blank

# JOINT DOCTRINE PUBLICATIONS HIERARCHY




All joint publications are organized into a comprehensive hierarchy as shown in the chart above. **Joint Publication (JP) 3-27** is in the **Operations** series of joint doctrine publications. The diagram below illustrates an overview of the development process:




JOINT
CHIEFS OF STAFF