Joint Publication 3-27

Homeland Defense

10 April 2018

PREFACE

1. Scope

This publication provides joint doctrine for homeland defense.

2. Purpose

This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff (CJCS). It sets forth joint doctrine to govern the activities and performance of the Armed Forces of the United States in joint operations, and it provides considerations for military interaction with governmental and nongovernmental agencies, multinational forces, and other interorganizational partners. 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 and executing their plans and orders. 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 objectives.

3. Application

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

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 CJCS, 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 US, 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:

KEVIN D. SCOTT
Vice Admiral, USN
Director, Joint Force Development

Intentionally Blank

SUMMARY OF CHANGES
REVISION OF JOINT PUBLICATION 3-27
DATED 29 JULY 2013

- **Reorganizes Chapter I, "Fundamentals of Homeland Defense," to describe homeland security (HS), defense support of civil authorities (DSCA), and homeland defense (HD) as a unified approach; adds more information on Department of Homeland Security's mission with respect to HS and the transregional, multi-domain, and multifunctional nature of the transnational threat environment; adds information on unmanned aircraft systems, global campaign plans, and incident awareness and assessment; updates laws, policies, and terminology; and enhances the succinctness of the chapter.**

- **Adds information to Chapter II, "Command Relationships and Interorganizational Cooperation," on unified action and properly defines United States Coast Guard's (USCG's) HD roles and the differences between maritime homeland security (MHS) and maritime homeland defense (MHD) tasks, as well as the required coordination between US Navy and USCG.**

- **Adds to Chapter II, "Command Relationships and Interorganizational Cooperation," US Alaskan Command and removes Joint Task Force–Alaska; clarifies US Pacific Command's role in HD and the MHD execute order; and updates terminology and references to other joint publications.**

- **Covers Chapter III, "Planning and Operations for Homeland Defense," operations in all domains for homeland defense; adds paragraph on MHS support to strategic sealift; aligns information operations as one of the seven joint functions; clarifies roles and responsibilities for homeland ballistic missile defense; expands cyberspace operations and critical infrastructure protection; and moves joint reception, staging, onward movement, and integration verbiage to more pertinent location.**

- **Updates Appendix A, "Relationships Betweeen Homeland Security, Homeland Defense and Defense Support of civil Authorities," to reflect changes made by National Defense Authorization Act Fiscal Year 2017 and adds a more concise diagram depicting the relationship between HS, HD, and DSCA.**

- **Revises the explanation and mission of multiple interorganizational agencies within the United States Government in Appendix B, "Facilitating Interorganizational Cooperation."**

- **Updates Appendix C, "North American Aerospace Defense Command Missions, Organization, and Structure," definitions and provides for a more succinct document.**

- **Updates references used throughout the document and removes extraneous descriptors for Appendix D, "References."**

Intentionally Blank

TABLE OF CONTENTS

GLOSSARY

FIGURE

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Discusses fundamentals of homeland defense (HD), to include threats; policy and legal considerations; active, layered defense; and the HD operational framework**
- **Describes command relationships and interorganizational cooperation in HD**
- **Outlines strategic guidance, operational factors, intelligence sharing, and joint functions considerations for planning and operations for homeland defense**

Fundamentals of Homeland Defense

The United States Government (USG) employs all instruments of national power to continuously detect, deter, prevent, and defeat threats to the homeland. This national imperative translates operationally into homeland security (HS), defense support of civil authorities (DSCA), and homeland defense (HD). The Department of Defense (DOD) is the lead federal agency (LFA) for defending against traditional external threats or aggression (e.g., nation-state conventional forces or weapons of mass destruction attack) and against external asymmetric threats that are outside of the scope of HS operations. The Department of Homeland Security (DHS) is the LFA for HS, and the United States Coast Guard (USCG) is the LFA for maritime homeland security (MHS). By law, DOD is responsible for two missions in the homeland: DSCA and HD.

HD is the protection of US sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression or other threats, as directed by the President of the US.

DOD executes HD by detecting, deterring, preventing, and defeating threats from actors of concern as far forward from the homeland as possible. HD is executed across the active, layered defense construct composed of the forward regions, the approaches, and the homeland. Commander, United States Northern Command (CDRUSNORTHCOM), and Commander, United

States Pacific Command (CDRUSPACOM), are the supported commanders for HD in their respective areas of responsibility (AORs), with all other combatant commanders (CCDRs) as supporting commanders.

Threats

The homeland is confronted by a variety of both disparate and interrelated threats that demand coordinated procedures and synchronized efforts among interagency partners responsible for law enforcement and national defense, particularly those who have overlapping roles, responsibilities, authorities, and capabilities.

Homeland Defense (HD) Policy and Legal Considerations

When conducted domestically, certain intelligence activities, military information support operations, rules of engagement (ROE), and rules for the use of force (RUF) have specific limitations, applications, and legal considerations.

Active, Layered Defense

Defending the homeland neither begins nor ends at US borders, so DOD planning is guided by the construct of an active, layered defense—a global defense that aims to deter and defeat aggression abroad and simultaneously protect the homeland. It is a defense-in-depth that relies on collection, analysis, and sharing of information and intelligence; strategic and regional deterrence; military presence in forward regions; and the ability to rapidly generate and project warfighting capabilities to defend the US, its allies, and its interests. This defense strategy integrates US capabilities in the forward regions of the world, in the geographic approaches to US territory, and within the US homeland.

The HD Operational Framework

The HD operational framework includes the plans and actions taken to detect, deter, prevent, shape, and defeat threats and aggression against the homeland. The purpose of HD is to protect against incursions or attacks on sovereign US territory, the domestic population, and critical infrastructure and key resources as directed.

Command Relationships and Interorganizational Cooperation

Virtually all the strategic threats to the homeland in United States Northern Command (USNORTHCOM) and United States Pacific Command (USPACOM) AORs are based in the AORs of other geographic combatant commanders (GCCs). This requires command relationships for a collaborative, federated architecture for targeting by USNORTHCOM and USPACOM with the Joint Staff J-2 [Intelligence Directorate]; the intelligence directorates of the combatant commands; the National Joint Operations and Intelligence Center; and other supporting CCDRs, especially those supporting GCCs in whose AORs those strategic threats reside.

Unified Action

Unified action is the synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort. In HD, this includes interaction with joint, single-Service, and multinational operations with the activities of other interagency partners, nongovernmental organizations (NGOs), international organizations, and the private sector to achieve unity of effort.

Command and Control Relationships and Responsibilities:

As stipulated in the Unified Command Plan (UCP), CDRUSNORTHCOM and CDRUSPACOM have specified tasks for HD activities. They are responsible for planning, organizing, and executing HD operations within their respective AORs. 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.

Geographic Combatant Commander Responsibilities

Functional Combatant Commander Responsibilities

Commander, United States Strategic Command (CDRUSSTRATCOM), is the lead CCDR for strategic deterrence planning and executes strategic deterrence operations, as directed.

US Cyber Command can support HD cyberspace operations (CO) in collaboration with USNORTHCOM, USPACOM, and DHS by coordinating activities within the required AOR

and assisting with expertise and capabilities directed and made available.

For operations conducted in the homeland, Commander, US Special Operations Command, serves as either a supported or supporting commander for selected counterterrorism activities and serves as a supporting commander to the GCCs with geographic HD responsibilities within their respective AORs.

For HD operations, Commander, US Transportation Command, provides, upon request, a director of mobility forces to advise on air mobility support operations

Interagency Coordination

HD operations are conducted in a complex operational environment (OE) that contains thousands of different jurisdictions (federal, state, tribal, and local), many agencies and organizations, the private sector, and several allies and multinational partners. From a USG perspective, this necessitates coordinated and integrated activities that have been previously exercised/rehearsed to facilitate effective interagency interoperability in addition to unity of effort. Coordination should be conducted through the defense coordinating officer/defense coordinating element of the affected region. The inherent interrelationships between HS, HD, and DSCA, and the potential for transition between those missions, creates a dynamic and complex environment in which interorganizational coordination and resulting interoperability could prove critical. From a DOD perspective, understanding and executing the multiple command relationships and organizational relationships required for simultaneous execution of HS, HD, and DSCA requires the utmost in interagency coordination.

Interorganizational Cooperation Considerations

HD mission response forces involve multiple organizations. Operation NOBLE EAGLE, the North American Aerospace Defense Command (NORAD), USNORTHCOM, and USPACOM operation aimed at defending the homeland, involves active duty personnel from the US Air Force, US Navy, the Canadian Forces, and National Guard members federalized for the

mission. These military forces coordinate with Department of Transportation (Federal Aviation Administration), DHS, the Department of Justice, and other USG departments and agencies.

Multinational Forces

To conduct the full range of HD operations, CCDRs should consider multinational and nonmilitary organizations. When a response force resides within an alliance, the procedures and structure of that alliance will normally determine the operational-level leadership. When a response force is based in a coalition (or a lead-nation structure in an alliance), the designated lead nation or other leadership mechanism will normally select the operational-level leadership. While the President and Secretary of Defense retain command authority over US forces, it is often prudent or advantageous to place appropriate US forces under the tactical control of a foreign commander for reasons such as maximizing military effectiveness and ensuring unity of effort.

Planning and Operations for Homeland Defense

Strategic Guidance

General strategy is provided in high-level policy documents such as the *National Security Strategy*, *Defense Strategy Review*, and the *National Military Strategy* (NMS). Similarly, high-level planning guidance is provided in the UCP; *Guidance for Employment of the Force* and Chairman of the Joint Chiefs of Staff Instruction 3110.01, *(U) Joint Strategic Capabilities Plan (JSCP).* Planning architecture is provided in Chairman of the Joint Chiefs of Staff Manual 3130.03, *Adaptive Planning and Execution Formats and Guidance.*

Operational Factors:

Civil and Military Relationships

Regardless of the size and scope of the particular operations, inevitably they will involve multiple jurisdictions (such as cities, counties, regions, tribes, and states). Managing such relationships will require significant time and effort on the part of federal, state, local, and tribal authorities to ensure proper coordination.

Commander's Communication Synchronization and Public Affairs

Joint force commanders (JFCs) are required to include communication goals and objectives in the commander's intent and to have a communication approach that ensures unity of themes, objectives, and messages among key activities; consistency in intent or effect between command operations, actions, and information; and a risk assessment of the information that may reach unintended audiences, create unintended consequences, and require risk mitigation measures.

Non-Department of Defense Federal, State, Territorial, Local, and Tribal Planning Factors

Interorganizational cooperation must occur between elements of DOD and non-DOD federal, state, local, and tribal agencies, as well as other participating USG departments and agencies for the purpose of achieving HD objectives.

Legal Considerations

Military operations inside the homeland can present unique and complex legal issues. Certain military functions (e.g., intelligence operations, ROE, and RUF) have specific applications and legal implications when conducted domestically. Coordination with the servicing office of the staff judge advocate for legal advice should be as early in the operation planning process as possible.

Intelligence Sharing for HD

The success of interorganizational cooperation in HD operations hinges upon timely and accurate information and intelligence. Information sharing environments should include as many essential participants as possible, understanding that not all are capable of participating in a collaborative environment. When possible, a collaborative intelligence sharing environment should be capable of generating and moving intelligence, operational information, and orders where needed in the shortest possible time.

Joint Fires

Joint fires may be provided to assist air, land, maritime, or special operations forces in conducting HD activities within an OE framed by complex legal authorities and significant interagency coordination. Although major operations against an enemy in the US remain highly unlikely, various threats require capabilities and preparations to deter or defeat them. For that

reason, the supported JFCs for HD have plans/orders for HD operations that anticipate the use of joint fires across the range of military operations.

Movement and Maneuver in the Conduct of HD:

HD land defense actions may include movement and maneuver, fires (for lethal and nonlethal effects), closing with and destroying an enemy, sustaining a joint force, and setting conditions for a return to peace.

Land Operations in the Conduct of HD

Specific HD land operations in support of HD may include security operations through force protection (FP) tasks or critical infrastructure protection (CIP). Defensive land operations will make use of existing USG departments' and agencies' capabilities where possible (e.g., DHS).

Maritime Operations in the Conduct of HD

Maritime operations in support of HD offer distinct challenges due to the nature of execution in or near the homeland in conjunction with interagency partners. DOD is the LFA for maritime HD and the USCG is the LFA for MHS. Through the relevant CCDR, DOD provides an active, layered defense; supports USCG MHS operations with DOD forces/capabilities; and defeats maritime threats to the homeland beyond the scope of MHS. Where coordination under the maritime operational threat response plan is required, issues such as designation of lead and supporting agencies, desired national outcome, required capabilities, asset availability, and authority to act must be determined.

Air Operations in HD Operations

NORAD is assigned the mission of aerospace control (including air sovereignty and air defense) of the airspace of the US and Canada. NORAD routinely maintains forces on alert for homeland air defense, cruise missile defense, and aerospace control alert missions against long-range incursions.

Space Operations in the Conduct of HD

To deter or preempt attacks and to protect military space assets, DOD conducts space operations in support of HD. These activities may serve to protect and defend the US's 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.

Cyberspace Operations in the Conduct of HD

The NMS for CO addresses three main roles: defense of the nation, national incident response, and CIP. GCCs with geographic HD responsibilities should ensure unified action at the theater level for CO. This includes coordinating with multinational and interagency partners as outlined in strategy, policy, and agreements.

Information Operations in the Conduct of HD

Information operations (IO) complements HD movement and maneuver in all domains by generating effects in the information environment that give the JFC a decisive advantage in any and all of its dimensions: physical, informational, and cognitive. IO also plays a significant role in the JFC's communication synchronization.

Movement in Support of HD

US Transportation Command can quickly assemble aircraft and flight crews for operations where expedited passenger movement is required. Surface transportation (commercial and organic) can be a viable option in those situations where the distance between the home station and the operational area is relatively short. Coordination with the National Guard Bureau is essential when using Air National Guard/Army National Guard assets for support of HD. In some instances, state and federal forces may be in the same operational area. Coordination between state and federal forces should occur to achieve unity of effort.

Protection

The protection function focuses on conserving the joint force's fighting potential in four primary ways: **active defensive measures, passive defensive measures, application of technology and procedures** to reduce the risk of friendly fire, and **emergency management and response** to reduce the loss of personnel and capabilities due to an all-hazards incident. It includes, but extends beyond, FP to encompass protection of US noncombatants; the forces, systems, and civil infrastructure of friendly nations; and other USG

departments and agencies, international organizations, and NGOs.

Sustainment:

Personnel

The core functional responsibilities of the manpower and personnel directorate of a joint staff are accomplished during any HD or other operation and are tailored to meet mission-specific requirements.

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 exceptions may apply to the USNORTHCOM AOR.

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 US. More specifically, the exceptions apply to the USNORTHCOM AOR.

Engineering

Military engineering support may be required simultaneously for HD and DSCA operations. The primary focus of the engineering effort will be to sustain and assist DOD forces employed in HD. The secondary effort will be DSCA, when requested and approved in accordance with DOD guidance and applicable plans.

Environmental Considerations

Military commanders employ environmentally responsible practices that minimize adverse impacts to human health and the environment. Plans will be developed to reduce or eliminate negative impacts on the environment and to minimize negative impacts to mission accomplishment caused by environmental degradation.

CONCLUSION

This publication provides joint doctrine for HD.

Intentionally Blank

CHAPTER I
FUNDAMENTALS OF HOMELAND DEFENSE

"…the Secretary, with the approval of the President and after consultation with the Chairman of the Joint Chiefs of Staff, shall provide, every two years or more frequently as needed, to the Chairman written policy guidance for the preparation and review of contingency plans, including plans for providing support to civil authorities in an incident of national significance or a catastrophic incident, for homeland defense, and for military support to civil authorities. Such guidance shall include guidance on the employment of forces, including specific force levels and specific supporting resource levels projected to be available for the period of time for which such plans are to be effective."

National Defense Authorization Act for Fiscal Year 2017

1. General

a. **The Homeland.** The US homeland is the physical region that includes the continental United States (CONUS), Alaska, Hawaii, US territories, and surrounding territorial waters and airspace. The United States Government (USG) employs all instruments of national power to continuously detect, deter, prevent, and defeat threats to the homeland. This national imperative translates operationally into homeland security (HS), defense support of civil authorities (DSCA), and homeland defense (HD). The Department of Defense (DOD) is the lead federal agency (LFA) for defending against traditional external threats or aggression (e.g., nation-state conventional forces or weapons of mass destruction [WMD] attack) and against external asymmetric threats that are outside of the scope of HS operations. The Department of Homeland Security (DHS) is the LFA for HS, and the United States Coast Guard (USCG) is the LFA for maritime homeland security (MHS). By law, DOD is responsible for two missions in the homeland: DSCA and HD.

b. HS, DSCA, and HD operations and events may occur simultaneously and require extensive coordination, integration, and synchronization. HS forms the foundation upon which the USG counters threats and hazards, consistent with Presidential Policy Directive (PPD)-8, *National Preparedness.* HS operations are constantly executed under legal authorities that enforce the rule of law at all levels of government in all areas subject to US jurisdiction, including the homeland and its approaches. DSCA and HD build upon the foundation of HS to counter the most sophisticated and/or nation-state threats that either exceed the scope of HS capabilities or require use of DOD authorities to defeat threats to the homeland. Considerations regarding simultaneous HS, DSCA, and HD operations are covered in more detail in Appendix A, "Relationships Between Homeland Security, Homeland Defense, and Defense Support of Civil Authorities."

(1) HS is an integrated concept developed as a result of the 11 September 2001 attacks on the US. The 2010 Quadrennial Homeland Security Review describes HS as the intersection of evolving threats and hazards with traditional governmental and civic responsibilities for civil defense, emergency response, law enforcement (LE), customs,

border control, and immigration. In combining these responsibilities under one overarching concept, HS breaks down longstanding stovepipes of activity that have been and could still be exploited by those seeking to cause harm. HS is a widely distributed and diverse national enterprise comprised of the collective efforts and shared responsibilities of federal, state, local, tribal, territorial, nongovernmental, and private-sector partners, individuals, families, and communities to maintain critical HS capabilities.

(a) DHS missions under the general concept of HS include the following:

1. Prevent terrorism and enhance security.

2. Secure and manage our borders.

3. Enforce and administer our immigration laws.

4. Safeguard and secure cyberspace.

5. Strengthen national preparedness and resilience.

For more information on DHS missions, see the 2014 Quadrennial Homeland Security Review *at* https://www.dhs.gov/quadrennial-homeland-security-review.

(b) DOD supports HS operations through DSCA and by providing DOD forces and capabilities to USCG MHS operations pursuant to 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* and applicable Secretary of Defense (SecDef) execute orders (EXORDs).

(c) DOD may also be required to participate in emergency preparedness (EP) under the National Preparedness System. EP includes 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 five preparedness mission areas under the National Response Framework (NRF). These five mission areas are prevention, protection, mitigation, response, and recovery. EP is considered a part of DOD's overall preparedness activities in support of the NRF. NRF is not a stand-alone activity, but is an integral part of DOD training, mitigation, and response for both HD and DSCA.

For more information on EP, see PPD-8, National Preparedness, *and the* National Response Framework *at https://www.fema.gov/national-response-framework.*

(2) DSCA is support provided by US federal military forces, DOD civilians, DOD contract personnel, DOD component assets, reserve and National Guard (NG) forces (when SecDef, in coordination with the governor[s] of the affected state[s], elect and request to use those forces under Title 32, United States Code [USC], Section 502) in response to requests for assistance from civil authorities for domestic emergencies, LE support, and other domestic activities or from qualifying entities for special events.

For more information on DSCA, see Joint Publication (JP) 3-28, Defense Support of Civil Authorities, *and Department of Defense Directive (DODD) 3025.18,* Defense Support of Civil Authorities.

(3) HD is the protection of US sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression or other threats, as directed by the President of the US.

(a) DOD executes HD by detecting, deterring, preventing, and defeating threats from actors of concern as far forward from the homeland as possible. DOD is responsible for the HD mission and leads the response with support from international partners and USG departments and agencies. HD is executed across the active, layered defense construct composed of the forward regions, the approaches, and the homeland. Commander, United States Northern Command (CDRUSNORTHCOM), and Commander, United States Pacific Command (CDRUSPACOM), are the supported commanders for HD in their respective areas of responsibility (AORs), with all other combatant commanders (CCDRs) as supporting commanders. CDRUSNORTHCOM and CDRUSPACOM are charged with specific responsibilities for HD and DSCA.

(b) CDRUSNORTHCOM is responsible for planning, organizing, and, as directed, executing HD operations within the United States Northern Command (USNORTHCOM) AOR in concert with missions performed by the North American Aerospace Defense Command (NORAD).

(c) CDRUSPACOM is responsible for planning and, as directed, executing HD operations within the United States Pacific Command (USPACOM) AOR.

(d) All other CCDRs, except Commander, United States Transportation Command (CDRUSTRANSCOM), are responsible for detecting, deterring, and preventing attacks against the US, its territories, and bases and, should deterrence fail, employ appropriate forces to defend the nation in forward regions and within the approaches to the homeland.

c. Within the homeland, HD, DSCA, and HS require pre-event and ongoing coordination with interorganizational and multinational partners to integrate capabilities and facilitate unified action. In this complex environment, there are numerous threats across multiple jurisdictions (i.e., federal, state, local, and tribal) that are addressed by a diverse group of actively involved stakeholders (e.g., international organizations, multinational partnerships, nongovernmental organizations [NGOs], and the private sector). DOD plans and prepares to operate in concert with other USG entities. For example, DOD operations may coincide with other actions to counter violent extremist threats, such as those of a hijacked commercial aircraft or attempts to perpetrate attacks using WMD. A coordinated approach to unified action promotes early identification of the desired USG objective(s) and subsequent coordination and collaboration with potential participants. Guidance such as the Maritime Operational Threat Response (MOTR) Plan is an example of this approach to operations.

For additional information, see JP 3-08, Interorganizational Cooperation.

For information regarding interagency roles, responsibilities, and required coordination protocols for conduct of air defense and maritime security operations to counter threats to the US, see the President-approved Aviation Operational Threat Response (AOTR) Plan *and the* MOTR Plan.

Specific guidance on interagency headquarters (HQ) planning and command center support of HD operations is contained in annex V (Interagency Coordination) of HD concept plans (CONPLANs) or operation plans (OPLANs).

2. Threats

a. HD should address all external threats and other threats (as directed by the President) to facilitate a broad-based defense-in-depth. An external threat or aggression is an action, incident, or circumstance that originates from outside of the homeland. Threats planned, prompted, promoted, caused, or executed by external actors may develop or take place inside the homeland. The reference to external threats does not limit where or how attacks may be planned and executed. The USG has sought to shape the international environment through the judicious application of diplomatic, informational, military, and economic instruments of national power. Given the persistent presence of both traditional nation-state and asymmetric threats, a proactive, comprehensive, and disciplined approach to HD is required. Additionally, military operations conducted in the homeland require an in-depth understanding of laws, policies, and procedures because of overlapping jurisdictions and legal authorities on the use of military forces.

b. The homeland is confronted by a variety of both disparate and interrelated threats that demand coordinated procedures and synchronized efforts among interagency partners responsible for LE and national defense, particularly those who have overlapping roles, responsibilities, authorities, and capabilities. Transnational threats have proven to be complex and enduring. A transnational threat is any activity, individual, or group not tied to a particular country or region that operates across international boundaries and threatens US national security or interests. Figure I-1 lists various aspects of the transnational threats to the homeland.

c. **WMD.** Adversaries have and continue to seek WMD and the means to deliver them to enhance their influence and achieve greater strategic leverage against US advantages. They may use the weapons to conduct an attack on US citizens, infrastructure, and other vital interests and to exploit US power projection, sustainment, and force protection (FP) vulnerabilities. Increased access to technology, materials, and expertise heightens the risk that threats will develop, proliferate, and use WMD to achieve their goals.

See JP 3-40, Countering Weapons of Mass Destruction, *for more information on WMD.*

Figure I-1. Homeland Defense Transnational Threat Environment

See JP 3-41, Chemical, Biological, Radiological, and Nuclear Response, *for more information on DOD actions and capabilities to mitigate the effects of a chemical, biological, radiological, and nuclear (CBRN) attack.*

d. **Adversaries.** The joint force faces an increasingly complex global security environment characterized by contested norms and persistent disorder. State and non-state adversaries seek to challenge the current international order by establishing new rules and norms that are unfavorable to our national interests. Weak states are increasingly incapable of maintaining domestic order, which permits other actors to employ violence in pursuit of their beliefs. Conflicts are increasingly transregional, multi-domain, and multifunctional (TMM) as adversaries' interests, influence, capabilities, and reach extend beyond single geographic areas. Additionally, the threat from individual actors and homegrown violent extremists, where an individual or small group of individuals executes attacks without any direct contact with a parent organization, has increased. These threats will continue to employ a variety of tactics, in particular, asymmetric employment of weapons, platforms, and information that could significantly affect not only the political-military balance, but potentially more significantly, the US economy and global trade.

3. Homeland Defense Policy and Legal Considerations

a. Multiple documents provide guidance for conducting HD operations. Specific planning factors, requirements, and objectives for HD operations are contained in plans associated with the HD mission.

b. **Special Considerations.** When conducted domestically, certain intelligence activities, military information support operations (MISO), rules of engagement (ROE), and rules for the use of force (RUF) have specific limitations, applications, and legal considerations. Further, ROE and RUF for domestic situations are often developed by less

institutionalized processes and can therefore potentially be less thorough and subjected to less rigor.

(1) **Posse Comitatus Act (PCA).** The PCA prohibits the use of the United States Army (USA) and United States Air Force (USAF) to participate in civilian LE within the homeland. Title 10, USC, also directs SecDef to promulgate regulations prohibiting members of the USA, United States Navy (USN), USAF, and United States Marine Corps (USMC) from providing direct assistance to civilian LE, which was accomplished in Department of Defense Instruction (DODI) 3025.21, *Defense Support of Civilian Law Enforcement Agencies*. HD is a Constitutional exception to the PCA. Military operations conducted as HD are not LE activities, and thus, Title 10, USC, forces are not subject to the restriction of the PCA. Additionally, several Act-of-Congress exceptions to the PCA permit the Armed Forces to support LE activities under other conditions. The PCA does not apply to NG forces under Title 32, USC, or state active duty status.

(2) **Intelligence Activities.** Intelligence activities refer to all activities that DOD intelligence components are authorized to undertake in accordance with (IAW) Executive Order (EO) 12333, *United States Intelligence Activities* (as amended); DODD 5240.01, *DOD Intelligence Activities;* Department of Defense Manual (DODM) 5240.01, *Procedures Governing the Conduct of DOD Intelligence Activities;* DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons;* Chief, National Guard Bureau (CNGB) Instruction 2000.01, *National Guard Intelligence Activities;* and CNBG Manual 2000.01, *National Guard Intelligence Activities.* Intelligence activities include the collection, retention, and dissemination of intelligence by DOD intelligence components.

(a) Intelligence activities conducted by US intelligence organizations in the US and its territories are strictly controlled. Several regulations and laws specifically govern the use of DOD intelligence assets and organizations in domestic operations. Figure I-2 lists several policy and guidance documents for the intelligence oversight program.

(b) **Acquisition of Open-Source Information.** 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 regardless of whether it is publicly available or not. Adherence to DODD 5240.01, DODM 5240.01, and DOD 5240.1-R, when performing such collections, is critical to the success of the effort and to avoid the appearance or conduct of questionable intelligence activities.

(c) **Acquisition of Information Concerning Persons and Organizations Not Affiliated with DOD.** Some restrictions on information gathering apply DOD wide, not just to DOD intelligence elements. 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

Guidance and Policy for the Intelligence Oversight Program

- Executive Order (EO) 12333, *United States Intelligence Activities* (as amended)
- Department of Defense Directive (DODD) 5148.11, *Assistant to the Secretary of Defense for Intelligence Oversight*
- Department of Defense Directive (DODD) 5240.01, *DOD Intelligence Activities*
- DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons*
- National Geospatial-Intelligence Agency's National System for Geospatial Intelligence Manual FA 1806, *Domestic Imagery,* Revision 5, March 2009, Administrative Update: May 2011
- North American Aerospace Defense Command and United States Northern Command Instruction 14-3, *Domestic Imagery,* 29 July 2014 modified 23 June 2016
- Department of Defense Manual (DODM) 5240.01, *Procedures Governing the Conduct of DOD Intelligence Activities*
- DOD Instruction 3115.12, *Open Source Intelligence (OSINT)*
- Chief, National Guard Bureau Instruction, 2000.01, *National Guard Intelligence Activities*
- Chief, National Guard Bureau Manual, 2000.01, *National Guard Intelligence Activities*

Figure I-2. Guidance and Policy for the Intelligence Oversight Program

outlined within the directive. DOD intelligence elements are not governed by this directive and must look to DODM 5240.01, *Procedures Governing the Conduct of DOD Intelligence Activities;* DODI 3115.12, *Open Source Intelligence;* DODD 5240.01, *DOD Intelligence Activities;* and DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons,* for guidance.

(d) **Domestic Use of Unmanned Aircraft Systems (UASs).** Unless specifically provided for in policy, law, or other guidance, SecDef approval is required for all domestic military UAS operations. Domestic use of UASs requires consultation with the Federal Aviation Administration (FAA) and must be consistent with applicable laws, regulations, and memoranda of agreement concerning the operations of UASs in the National Airspace System.

For more details regarding domestic use of UASs, refer to Deputy Secretary of Defense Policy Memorandum 15-002, Guidance for the Domestic Use of Unmanned Aircraft Systems. *For additional details, refer to Deputy Secretary of Defense Memorandum 16-003,* Countering Small Unmanned Aircraft Systems in the Homeland.

(e) **Incident Awareness and Assessment (IAA) Products.** In support of the LFA and civil authorities in a HD or DSCA mission, SecDef authorizes the use of traditional intelligence capabilities of DOD intelligence component assets for non-intelligence purposes to provide IAA for the following missions: situational awareness, damage assessment, evacuation monitoring, search and rescue, CBRN assessment, hydrographic survey, and dynamic ground coordination. IAA should be performed by

DOD assets only when such actions cannot be performed by local entities or other USG departments and agencies in a timely manner.

For more information on IAA, refer to JP 3-28, Defense Support of Civil Authorities, *and the Chairman of the Joint Chiefs of Staff (CJCS) Standing DSCA EXORD.*

Details on intelligence support to HD can be found in JP 2-0, Joint Intelligence.

(3) **MISO.** MISO are not conducted against US persons IAW law and DOD policy. However, in addition to HD activities outside of the US homeland, as part of the discussion in paragraph 5, "The Homeland Defense Operational Framework," military information support forces and equipment may also be used to conduct civil authority information support (CAIS) activities during domestic emergencies within the boundaries of the US homeland. A CAIS element supports the designated primary agency or civil authority to disseminate information during domestic emergencies (whether relating to national security or disaster relief operations). CAIS activities are not part of any MISO program. The Joint Staff issues specific guidance for military information support forces, as well as the designated command and control (C2) authority for the mission-tailored CAIS component.

See JP 3-13.2, Military Information Support Operations, *for a more complete discussion on MISO.*

(4) **ROE and RUF.** US forces, when performing an HD mission, must be prepared to engage the enemy IAW the appropriate ROE and RUF.

(a) ROE are directives issued by competent military authorities which delineate the circumstances and limitations under which US forces will initiate or continue combat engagement with other forces encountered. **Standing rules of engagement (SROE) apply to air and maritime HD missions conducted within the US, its territories, or territorial seas, unless otherwise directed by SecDef.** Supplemental ROE may be necessary to meet mission-specific ROE requirements and are submitted by the appropriate commander.

See Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3121.01, (U) Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces, *for additional information.*

(b) RUF are directives issued to guide US forces on the use of force during various operations. The standing rules for the use of force (SRUF) apply to land HD missions occurring within US territory and to DOD forces, civilians, and contractors performing LE and security duties at all DOD installations (and off-installation, while conducting official DOD security functions), 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 the CJCS for SecDef approval.

(c) ROE and RUF must conform to appropriate laws, including federal law (to include military law), the law of war, and other relevant international laws, and they

must conform to the situation and locality involved. When NG forces are in state active duty or Title 32, USC, status, the state RUF will apply. **Commanders are responsible for the education and training of their personnel on ROE, RUF, and the use of nonlethal and lethal force before they deploy from home station to perform a DSCA or HD mission.** Escalation of force (i.e., moving from nonlethal to lethal force as the situation dictates) also needs to be part of the training. 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 ROE or RUF.

c. Commanders consider a variety of weapons, to include nonlethal weapons and capabilities. Nonlethal capabilities may provide an effective alternative means of employing force to reduce the probability of death or serious injury to civilians or belligerents, as well as decrease the possibility for collateral damage. **Employment of nonlethal capabilities must be considered for inclusion in HD plans, ROE, and RUF.** Additionally, commanders plan and conduct rehearsals that test and exercise the adequacy of planned ROE and RUF and prepare their personnel for HD operations.

Additional information on the employment of nonlethal capabilities can be found in DODD 3000.03E, DOD Executive Agent for Non-Lethal Weapons (NLW), and NLW Policy; *Army Techniques Publication (ATP) (Field Manual [FM] 3-22.40)/Marine Corps Tactical Publication (MCTP) 10-10A (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/Coast Guard Tactics, Techniques, and Procedures (CGTTP) 3-93.2,* Multi-Service Tactics, Techniques, and Procedures for the Employment of Nonlethal Weapons; *and Army Training Circular 3-19.5,* Nonlethal Weapons Training. *USNORTHCOM guidance on the use of nonlethal capabilities can be found in* USNORTHCOM OPORD [Operation Order] 01-13.

4. Active, Layered Defense

a. Defending the homeland neither begins nor ends at US borders, so DOD planning is guided by the construct of an active, layered defense—a global defense that aims to deter and defeat aggression abroad and simultaneously protect the homeland. It is a defense-in-depth that relies on collection, analysis, and sharing of information and intelligence; strategic and regional deterrence; military presence in forward regions; and the ability to rapidly generate and project warfighting capabilities to defend the US, its allies, and its interests. This defense strategy 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.** In the forward regions outside US territories, the objective is to detect, prevent, shape, or when necessary, defeat threats to the US. Actions may include combat operations; security cooperation; military engagement activities; peace operations; intelligence operations; or preemptive measures such as direct action missions, cyberspace operations (CO), or global strike.

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. The *National Military Strategy* (NMS) emphasizes the importance of joining the efforts of multinational and interagency partners to form an integrated defense. Protecting these approaches requires intelligence and, when possible, enhanced, persistent surveillance that allows the US to detect, track and, if required, interdict and defeat potential threats.

d. **The Homeland.** If deterring or 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 forward regions and/or the approaches.

5. The Homeland Defense Operational Framework

a. The HD operational framework includes the plans and actions taken to detect, deter, prevent, shape, and defeat threats and aggression against the homeland. The purpose of HD is to protect against incursions or attacks on sovereign US territory, the domestic population, and critical infrastructure and key resources (CI/KR) as directed. The following are DOD HD objectives:

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

(2) Ensure defense of the homeland and deny a threat's access to the nation's sovereign airspace, territory, and territorial seas.

(3) Ensure access to cyberspace and information (including information systems and security).

(4) Protect the domestic population and critical infrastructure.

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

(6) Decisively defeat any attack if deterrence fails.

(7) Recover the military force to restore readiness and capabilities after any attack or incident.

b. The diversity of threats requires DOD, the military instrument of national power, take a broad role to coordinate all the requirements and objectives of the HD operational framework. HD operations require integration of capabilities and synchronization of activities (i.e., arrangement of activities across time, space, and purpose) through interagency coordination, and, when necessary, interorganizational coordination.

c. DOD conducts activities and operations globally to contribute to national preparedness and defense of the homeland. They are carried out in various operational environments (OEs). An OE encompasses physical areas of the air, land, maritime, and

space domains; the information environment (which includes cyberspace); the electromagnetic spectrum; and other factors. HD operations are conducted IAW laws; treaties and international agreements; national authorities; and DOD, CJCS, Military Department, and Service policy and doctrine. HD operations require active and passive defenses, and DOD may conduct offensive actions (to include preemptive activities) to deter, disrupt, and destroy enemy capabilities before they can be offensively employed.

(1) Outside the US (in the forward regions and approaches), DOD conducts activities to maintain the freedom to operate in portions of the OE, access information, and conduct operations or campaigns to disrupt and defeat terrorists and other enemies before they are able to execute attacks against the US homeland. Per CJCSI 3110.01, *(U) Joint Strategic Capabilities Plan (JSCP),* HD must be integrated into the global campaign plans. Identity activities are used to restrict mobility and access. Collected identity information and identity intelligence analytical methodologies are leveraged to identify threat actors and produce widely releasable products to support targeting, tactical screening, vetting, and FP initiatives that support global operations, HD, national security screening, and vetting activities by interagency partners. DOD security cooperation activities (e.g., exercises, exchanges) and counterproliferation and nonproliferation activities also advance working relationships, gain or maintain access to a partner nation (PN), and increase interoperability with friends and allies. The DOD State Partnership Program (SPP) contributes to these initiatives and is part of the GCCs' security cooperation program.

See Joint Doctrine Note (JDN) 2-16, Identity Activities, *for more information on identity information and identity intelligence.*

(2) Within the homeland, military activities are conducted in, or adjacent to, the land mass, airspace, and territorial waters of the US. These activities require freedom of action and full access and use of capabilities in cyberspace and space. HD includes ballistic missile defense (BMD); cruise missile (CM) defense; interdiction; land operations, to include protection of critical infrastructure; and defensive cyberspace operations (DCO). The defense of the homeland requires a multi-domain approach.

d. **HD operations require thorough preparation.** DOD EP activities at the strategic level may focus on actions associated with continuity of operations (COOP), continuity of government (COG), and national preparedness. At the operational level, however, DOD emergency preparations to defend the homeland include activities such as joint and interagency interoperability and coordination, joint training exercises and experimentation, and development of information and intelligence sharing architectures.

e. **Early detection facilitates timely identification, tracking, and engagement decisions for threats before they reach the homeland.** In the forward regions and approaches, intelligence and, when possible, persistent intelligence, surveillance, and reconnaissance can provide decision makers with possible warnings, early warning, and assessments. CONUS airspace is protected in part by NORAD's integrated tactical warning and attack assessment (ITW/AA) functions. For maritime domain awareness, the National Maritime Intelligence-Integration Office is an interagency organization that works at the national and international levels to facilitate the integration of maritime

information and intelligence collection and analysis in support of national policy and interagency decision makers at all levels of the USG. Additionally, maritime warning utilizes mutual support agreements with other commands and agencies responsible for maritime defense and security to enable identification, validation, and response to threats to North America. Another essential interagency organization is the National Counterterrorism Center (NCTC) that has the specific and unique mission to acquire, integrate, analyze, and disseminate all available USG information about terrorist threats and identities. The US and its multinational partners seek a global awareness of all threats to national security, individually and collectively, to increase the ability to deal with a range of threats at home and abroad. Early detection of CBRN threats emanating from any theater must be integrated throughout intelligence planning and execution from collection to dissemination.

f. **Deterrence is a key HD objective.** Deterrence is the prevention of adversary actions contrary to enduring national interests of the US, by the existence of a credible threat of unacceptable consequences. Credible deterrence operates by influencing adversary decision making through the demonstration of US capability and strategic messaging of US resolve to employ capabilities to not only deny the adversary any benefits from taking action, but also to impose costs from taking action. USG offensive capabilities coupled with defensive measures and DOD EP activities may deter an adversary from threatening or attacking the homeland. Adversaries must understand USG capabilities, to include the reliability and readiness of well-trained, equipped, and rapidly deployable forces. Therefore, deterrence is fundamentally about shaping adversary perceptions to believe that the cost of action, or inaction, outweighs perceived benefits. See JP 3-0, *Joint Operations,* for additional information on deterrence.

g. **DOD must be prepared to rapidly act offensively or defensively against threats and aggression.** DOD, as directed by the President, may conduct preemptive and/or active defense actions including flexible deterrent options and flexible response options IAW international and domestic law, national policy, and directives. If deterrence fails, the objective of these operations is to destroy, degrade, disrupt, or neutralize weapons; launch platforms; support command, control, and communications; logistics; and intelligence collection capabilities before they are employed by a threat. Examples of offensive operations may include global strikes, direct action, and offensive space control. The US and its multinational partners work together to synchronize activities and measures that may include any or all of their instruments of national power.

h. **Primary HD defensive actions** include active and passive measures to defeat threats already deployed or en-route to a target. Active defenses employ defensive actions (e.g., defensive counterair) and offensive actions (e.g., counterattacks) to deny a contested area or position to the enemy and are designed to reduce the effectiveness of or stop attacks on US sovereign territory, domestic population, and CI/KR. Active defenses employ land, maritime, air, space, cyberspace, and special operations forces assets. This multi-domain approach increases the reach of active defenses. The objective of HD passive defense is to reduce the probability of, and minimize the damage caused by, hostile actions. Passive defenses include FP and critical infrastructure risk mitigation actions to reduce targeting

effectiveness. They also include deception, mobility, dispersion, systems hardening and protective construction, warning and surveillance, and operations security.

Intentionally Blank

CHAPTER II
COMMAND RELATIONSHIPS AND INTERORGANIZATIONAL COOPERATION

1. General

a. HD is part of a global active, layered defense-in-depth that aims to deter and defeat aggression abroad and simultaneously protect the homeland. It includes the forward regions, the approaches, and the homeland. The relationships of participants for some HD activities/operations may be simple and others may be complex, but the supported joint force commander (JFC) is responsible for all participants understanding their established command and organizational relationships for the unity of command and interorganizational cooperation required for unified action during an HD operation.

b. 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. CCDRs prescribe the chain of command within their commands and designate the appropriate authority to be exercised by subordinate commanders. Dependent upon the location and type of threat to the homeland, CDRUSNORTHCOM and/or CDRUSPACOM would be designated as a supported CCDR for HD.

For more details regarding establishment of support relationships and responsibilities of supported and supporting CCDRs, see JP 1, Doctrine for the Armed Forces of the United States.

c. A consideration that significantly affects command relationships for HD is that virtually all the strategic threats to the homeland in USNORTHCOM and USPACOM AORs are based in the AORs of other GCCs. This requires command relationships for a collaborative, federated architecture for targeting by USNORTHCOM and USPACOM with the Joint Staff J-2 [Intelligence Directorate]; the intelligence directorates of the combatant commands (CCMDs); the National Joint Operations and Intelligence Center; and other supporting CCDRs, especially those supporting GCCs in whose AORs those strategic threats reside.

For more details regarding the relationships and process for federated targeting support, see JP 3-60, Joint Targeting.

2. Unified Action

a. Unified action is the synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort. In HD, this includes interaction with joint, single-Service, and multinational operations with the activities of other interagency partners, NGOs, international organizations, and the private sector to achieve unity of effort. Because of the normal multitude of interorganizational partners and other participants, HD is essentially a model of unified action, especially with regard to how forces and other organizations can coordinate and operate day-to-day in the same OE.

b. Canadian forces work with US forces to provide aerospace warning concerning North America through NORAD. In the context of NORAD's missions, "North America" means Alaska, Canada, CONUS, Puerto Rico, and the US Virgin Islands, including the air defense identification zones, the air approaches, maritime areas, internal navigable waterways, and the maritime approaches thereto. In the US, DOD, through NORAD, defends against air threats—including manned aircraft, unmanned aircraft (UA), and CMs—whether in the approaches or within US airspace. While DOD has sole responsibility for defeating air threats, it receives assistance from the FAA and DHS assets for early identification of anomalous air activity which may ultimately threaten the US. The Air National Guard (ANG) supports HD on a daily basis with alert aircraft to rapidly establish air dominance within US airspace. The Army National Guard (ARNG) supports HD on a daily basis on alert while conducting missile defense operations within US airspace.

c. During preparation for potential HD land operations, specific USA, USMC, and special operations units, in conjunction with USNORTHCOM and USPACOM components and subordinate unified commands, coordinate and conduct exercises with DHS and other interagency partners. ARNG may support HD as a functionary of the individual states and territories under Title 32, USC, status or in state active duty status. The USA and USMC interact with mission partners through civil-military operations centers (CMOCs) or state emergency management agencies staffed with an emergency preparedness liaison officer (EPLO). The CMOC capability is established and manned by civil affairs personnel, but works best when tailored to the specific task associated with the mission and augmented by assets (e.g., engineer, medical, transportation) available to the supported commander and unified action partners to synchronize resources, personnel, and stabilization efforts. The components and subordinate unified commands also work with Canadian forces to conduct a cooperative defense to secure the land approaches supporting in-depth defense of the homeland. Command relationships and interagency coordination required for the complex OE for HD are planned and routinely rehearsed in national-level exercises.

d. The Royal Canadian Navy teams with USN (i.e., US Naval Forces, Northern Command) and USCG forces through cooperative training and combined exercises to ensure both nations' maritime forces and agencies are poised to respond to maritime threats to either nation. In the US, DOD has the lead for HD, but many USG departments and agencies are partners in a collaborative approach.

e. The use of civilian and military space capabilities is essential to the effectiveness of conducting HD. Canadian forces work with US forces to provide aerospace warning of space and missile attack through the NORAD Agreement. The Joint Functional Component Command for Space (JFCC Space) at United States Strategic Command (USSTRATCOM) and the Service space forces conduct operations to protect and defend the right to operate in space and are responsible for securing DOD critical assets in space. GCCs with HD responsibilities provide FP for those ground-based space assets located in their respective AORs. USSTRATCOM and JFCC Space coordinate with the CJCS, other CCMDs, DOD, other USG departments and agencies (e.g., Defense Information Systems

Agency [DISA]), the National Aeronautics and Space Administration, commercial partners, and international agencies to integrate civil and military space assets.

f. For **cyberspace,** the vulnerability and complex interrelationship of national and international networks demand closely coordinated action among the military, private sector, and other government entities at all levels. CCMD CO support staff, the Services, and United States Cyber Command (USCYBERCOM) are the military front line of defense. DHS has the responsibility for securing US cyberspace at the national level by protecting non-DOD USG networks against cyberspace intrusions and attacks. Within DHS, the Office of Cybersecurity and Communications (CS&C) is tasked to protect USG network systems from cyberspace threats. USPACOM and USNORTHCOM, because of their HD and DSCA responsibilities, have unique coordination requirements for CO through their CO support staff with USCYBERCOM.

For more information on operations in cyberspace, see JP 3-12, Cyberspace Operations.

3. Command and Control Relationships and Responsibilities

a. Military forces remain under control of the established chain of command when conducting HD operations. IAW with DODD 3160.01, *Homeland Defense Activities Conducted by the National Guard*, in exceptional circumstances, NG forces may conduct HD activities in a state active duty or Title 32, USC, status. These NG forces may subsequently transition to Title 10, USC, status as authorized by law.

(1) **SecDef.** SecDef is the President's principal assistant in all matters related to DOD. Subject to the direction of the President and law, SecDef has authority, direction, and control over DOD. Unless otherwise directed by the President, the operational chain of command runs from the President to SecDef and from SecDef to the CCDRs.

(2) **Assistant Secretary of Defense (Homeland Defense and Global Security) (ASD[HD&GS]).** The ASD(HD&GS), under the authority, direction, and control of the Under Secretary of Defense for Policy (USD[P]), serves as the principal civilian advisor to SecDef and the USD(P) on HD activities, DSCA, and Western Hemisphere security matters. The ASD(HD&GS) provides overall supervision of HD activities of DOD pursuant to Title 10, USC, Section 138. These activities include, but are not limited, to the Defense Critical Infrastructure Program (DCIP), domestic antiterrorism (AT), the Defense Continuity Program, the Emergency Management Program, other HD-related activities, and alignment of HD policies and programs with DOD policies for counterterrorism (CT) and counternarcotics. The ASD(HD&GS) provides DOD policy and guidance for the following:

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

(b) DCIP. (See DODI 3020.45, *Defense Critical Infrastructure Program [DCIP] Management.)*

(c) DOD domestic AT IAW DODI 2000.12, *DOD Antiterrorism (AT) Program.*

(d) DOD domestic CT activities, except those executed by special operations forces (SOF). (See DODD 5111.13, *Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs [ASD{HD&ASA}]*.)

(e) DOD continuity-related activities, to include COOP, COG, and enduring constitutional government, are managed under the Defense Continuity Programs. (See DODD 3020.26, *Department of Defense Continuity Programs.)*

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

(3) **CJCS.** As senior military advisor to the President, the National Security Council (NSC), the Homeland Security Council (HSC), and SecDef, the CJCS has numerous responsibilities relating to HD and DSCA. 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 strategic plans, including those which conform to resource levels projected by SecDef. The CJCS also provides for the preparation and review of contingency plans, which conform to policy guidance from the President and SecDef. The CJCS reviews HD plans and operations for compatibility with other military plans and assists CCDRs in meeting their operational requirements. Finally, IAW established DOD policy, the CJCS reviews and assesses requests from governors for NG HD activities and provides recommendations to SecDef.

(4) **Joint Chiefs of Staff (JCS).** The JCS is made up of the CJCS; the Vice CJCS; the Chiefs of Staff of the Army and Air Force; the Chief of Naval Operations; the Commandant of the Marine Corps; and the CNGB. While the CJCS is the senior military advisor, the other members of the JCS are military advisors to the President, the NSC, the HSC, and SecDef, as well. A member of the JCS may submit to the CJCS advice or an opinion in disagreement with, or in addition to, the advice or opinion presented by the CJCS. If a member submits such advice or opinion, the CJCS shall present that advice or opinion to the President, NSC, HSC, or SecDef at the same time that he presents his own advice. The individual members of the JCS may also provide advice when specifically requested.

(5) **Commandant, USCG.** The Commandant of the USCG advises the JCS on matters related to HD, HS, and DSCA from the USCG perspective and, as a force provider, allocates forces under Title 10, USC. The USCG's supporting roles in HD include maritime interception and interdiction operations, port security and harbor defense, coastal sea control, MOTR support, and protection in cyberspace. The Secretary of Homeland Security delegated authority to the Commandant, USCG, to conduct all MHS activities, and the Commandant, USCG, conducts MHS under Title 14, USC, authority, through area, district, and sector commanders. Pursuant to the *Memorandum of Agreement Between the Department of Defense and Department of Homeland Security for the Inclusion of the US*

Coast Guard in Support of Maritime Homeland Defense, Commanders Atlantic Area and Pacific Area continuously exist within DOD as Commander, Coast Guard Defense Force (CGDEFOR), East and West, respectively. USCG forces must maintain a state of readiness to rapidly transition from carrying out MHS roles and missions under Title 14, USC, and the C2 of USCG commanders to execute specific maritime homeland defense (MHD) tasks under Title 10, USC, and the C2 of CGDEFOR.

(6) **CNGB.** The CNGB serves as a principal advisor to SecDef, through the CJCS, on matters involving non-federalized NG and on other matters as determined by SecDef. As the principal advisor to the Secretary of the Army and the Secretary of the Air Force on NG matters, the CNGB assists the state adjutants general in supporting, synchronizing, and facilitating NG HD activities.

(7) **Governors of the States.** Governors retain C2 of state NG forces executing HD activities in their respective states IAW Title 32, USC, Sections 901-908. The President, SecDef, and CCDRs are not in the state operational chain of command. However, SecDef may set conditions for authorization of Title 32, USC, Section 902. Governors coordinate with the National Guard Bureau (NGB) to facilitate NGB synchronization of state HD activity planning with the appropriate CCDRs to ensure NG-funded, Title 32, USC, Section 902, HD activities do not conflict with ongoing federal missions. Governors and state adjutants general are not in the federal operational chain of command.

b. **GCC Responsibilities.** The Unified Command Plan (UCP) establishes CCMDs' missions, responsibilities, AORs, and functions. As stipulated in the UCP, CDRUSNORTHCOM and CDRUSPACOM have specified tasks for HD activities (these commanders are referred to subsequently in this publication as GCCs with geographic HD responsibilities). They are responsible for planning, organizing, and executing HD operations within their respective AORs. 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 bi-national command composed of Canadian and US forces. Per the NORAD Terms of Reference, NORAD's primary missions are aerospace warning, aerospace control, and maritime warning for North America. CDRNORAD is responsible to the Canadian government and USG, communicating through the Chief of Defence Staff (CDS) (Canada) and CJCS, respectively. CDRUSNORTHCOM is normally designated as CDRNORAD. IAW the NORAD Agreement, when CDRNORAD is a Canadian, CDRUSNORTHCOM will be designated Deputy Commander NORAD. While NORAD and USNORTHCOM have separate missions defined by separate authorities, parts of the USNORTHCOM AOR overlap with NORAD's operational area (OA) (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 is a part of the other. However, their operational focus runs parallel with detecting, deterring, preventing, and defeating threats and aggression in the air approaches and airspace of North America. NORAD is supported by the Canadian

Joint Operations Command (CJOC), USNORTHCOM, USPACOM, and United States Southern Command (USSOUTHCOM) in the conduct of missions assigned to NORAD. NORAD's maritime warning mission supports CJOC, USNORTHCOM, USPACOM, and USSOUTHCOM in their assigned missions to defend North America. NORAD warns of maritime threats to or against North America to enable identification, validation, and response by national commands and agencies responsible for maritime defense and security.

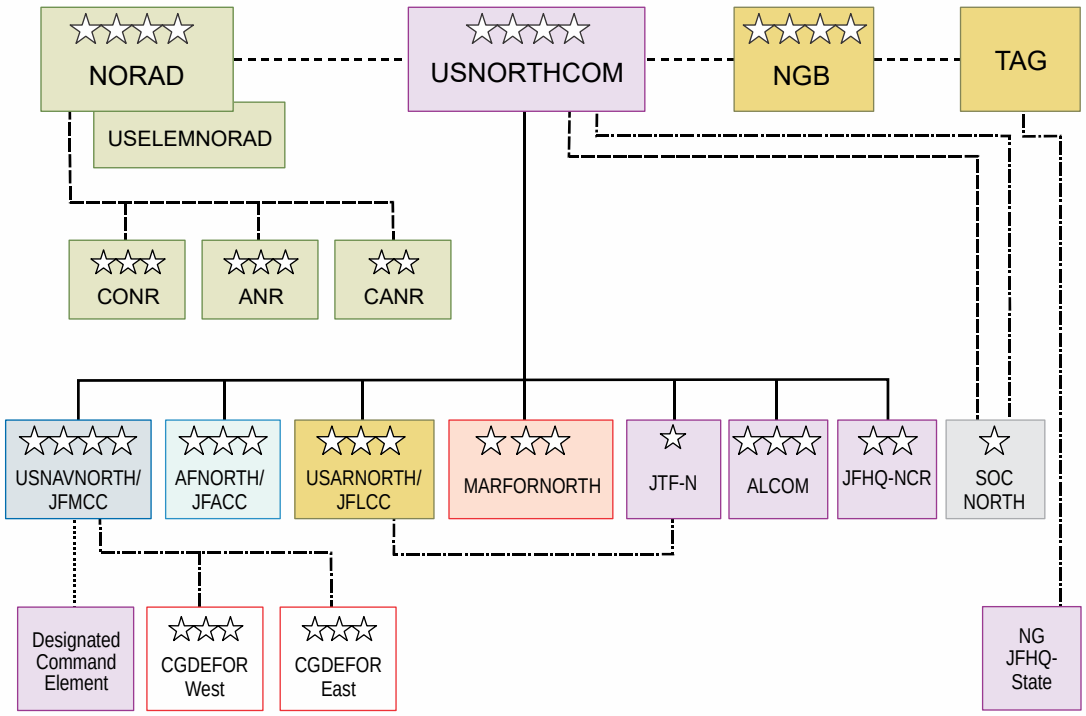
See Appendix C, "North American Aerospace Defense Command, Missions, Organization, and Structure," for detailed information on NORAD.

(2) **CDRUSNORTHCOM.** As directed by the President, CDRUSNORTHCOM conducts military operations within the USNORTHCOM AOR utilizing forces to detect, deter, or defeat an incursion into US sovereign territory. CDRUSNORTHCOM has COCOM over USA, USAF, USN, and USMC Service component command HQs and operational control (OPCON) over the theater special operations command (TSOC). When forces are OPCON to the command for HD operations, the deployment order or EXORD will normally establish command relationships. CDRUSNORTHCOM, normally designated a supported commander for HD, determines the appropriate C2 structure to employ these forces. CDRUSNORTHCOM may retain direct C2 of forces as the 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-1 provides the USNORTHCOM HD command relationships.

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

(a) **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 USA and USMC. 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, United States Army, North (CDRUSARNORTH), is designated as the joint force land component commander (JFLCC) for USNORTHCOM and has a main command post and deployable contingency command post that can, with augmentation, quickly become a full JTF. United States Army, North (USARNORTH) has the mission to conduct HD operations for USNORTHCOM, but current USA doctrine stipulates that division and corps HQs provide C2 for USA units conducting major combat operations, not theater USA operations. Nevertheless, the homeland is a unique theater of operations for the USA with special requirements, so USARNORTH could request that state NG units provide assistance for HD activities. USARNORTH could then focus on the theater opening and sustainment operations for all ground forces participating in an HD mission in the homeland.

United States Northern Command Homeland Defense Command Relationships



Legend

AFNORTH	Air Force North
ALCOM	United States Alaskan Command
ANR	Alaskan North American Aerospace Defense Command Region
CANR	Canadian North American Aerospace Defense Command Region
CGDEFOR	Coast Guard defense force
CONR	continental United States North American Aerospace Defense Command Region
JFACC	joint force air component commander
JFHQ-NCR	Joint Force Headquarters-National Capital Region
JFLCC	joint force land component commander
JFMCC	joint force maritime component commander
JTF-N	Joint Task Force-North
MARFORNORTH	United States Marine Corps Forces, North
NGB	National Guard Bureau
NG JFHQ-State	National Guard joint force headquarters-state
NORAD	North American Aerospace Defense Command
SOCNORTH	United States Special Operations Command, North
TAG	the adjutant general
USARNORTH	United States Army, North
USELEMNORAD	United States Element, North American Aerospace Defense Command
USNAVNORTH	United States Naval Forces, Northern Command
USNORTHCOM	United States Northern Command

———	combatant command (command authority)
·····	supporting
—·—·—	operational control
- - - - -	coordination
———	direct support

Figure II-1. United States Northern Command Homeland Defense Command Relationships

(b) **C2 for HD Maritime Operations in the USNORTHCOM AOR.** Commander, United States Naval Forces, Northern Command (COMUSNAVNORTH), is

the component commander to CDRUSNORTHCOM and has been designated as the joint force maritime component commander (JFMCC). COMUSNAVNORTH conducts MHD operations in the USNORTHCOM AOR and supports USCG MHS operations. Upon declaration of an MHD mission in the USNORTHCOM AOR, the USCG allocates forces to USNORTHCOM, when requested, for execution of JFMCC-assigned tasks under the C2 of CGDEFORs East and West. USCG forces allocated to USNORTHCOM for MHD tasking may be attached with specification of tactical control (TACON) of the JFMCC, to USNORTHCOM, or OPCON if mutually agreed with the USCG. Figure II-2 depicts the applicable MHD and MHS command relationships.

(c) **C2 for HD Air Operations in the USNORTHCOM AOR.** C2 for HD air operations in the USNORTHCOM AOR is complex. Where the NORAD OA and the USNORTHCOM AOR overlap, NORAD normally retains authority for the aerospace control and aerospace warning missions. The Commander, Continental United States North American Aerospace Defense Command Region (CONR), is appointed the Combined Force Air Component Commander for CONUS, the Virgin Islands, and Puerto Rico. For US-only air operations within CONUS, the Commander, Air Force North (CDRAFNORTH), is designated the joint force air component commander (JFACC). CDRAFNORTH is dual-hatted as the Commander, CONR. For US-only air operations in Alaska, the commander of the combined US-Canadian Alaskan North American Aerospace Defense Command Region (ANR) may be designated the JFACC. Close coordination between the JFACC(s) and NORAD is essential for synchronization of operations.

(d) **C2 for HD Space Operations in the USNORTHCOM AOR.** USSTRATCOM conducts space operations in direct support to USNORTHCOM's HD operations. Commander, United States Strategic Command (CDRUSSTRATCOM), has designated coordinating authority to Commander, JFCC Space, for the planning of space operations in operational-level support of USSTRATCOM's UCP missions. Commander, JFCC Space, integrates military, intelligence, civil, and commercial space requirements between CDRUSSTRATCOM and CDRUSNORTHCOM. CDRUSNORTHCOM has designated CDRAFNORTH as USNORTHCOM's space coordinating authority (SCA) with primary responsibility for joint space operations planning, to include ascertaining space requirements in support of USNORTHCOM's HD operations. CDRUSNORTHCOM or CDRUSSTRATCOM may prescribe direct liaison authorized (DIRLAUTH) between SCAs to ensure prompt and timely support.

(e) **C2 for HD CO in the USNORTHCOM AOR.** CDRUSNORTHCOM is responsible for defending against, mitigating, and defeating cyberspace threats against USNORTHCOM and NORAD missions that are not associated with the defense of the Department of Defense information network (DODIN) in coordination with USCYBERCOM and USPACOM. USNORTHCOM will plan and execute CO during HD in coordination with USCYBERCOM. Finally, geographic and functional CCDRs, as well as the Services, are responsible for protecting their networks located within the USNORTHCOM AOR which are not specifically assigned or attached to USNORTHCOM.

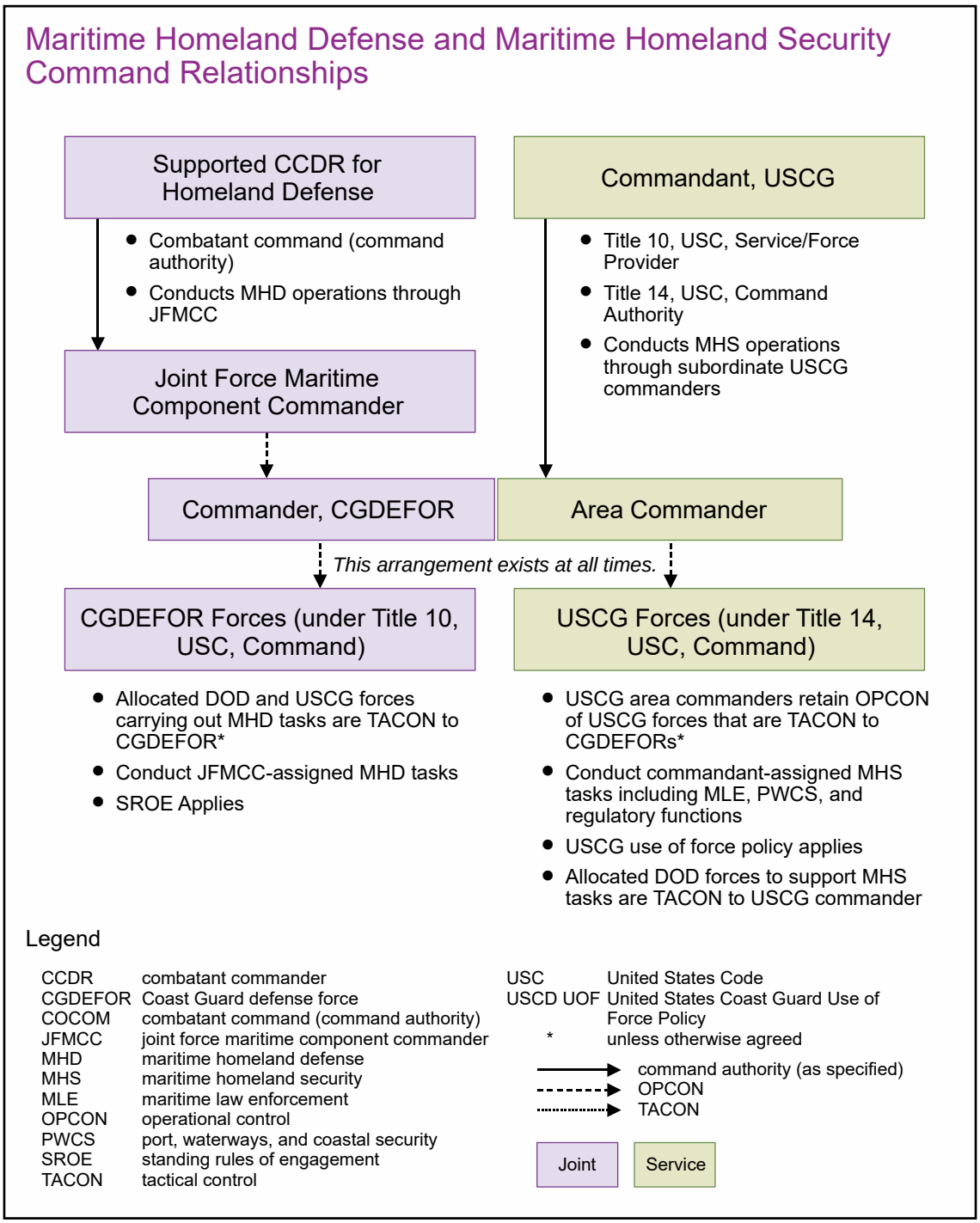


Figure II-2. Maritime Homeland Defense and Maritime Homeland Security Command Relationships

For more information on CO, see JP 3-12, Cyberspace Operations.

(f) **C2 for HD Special Operations in the USNORTHCOM AOR.** United States Special Operations Command, North (SOCNORTH) is under COCOM of Commander, United States Special Operations Command (CDRUSSOCOM), and OPCON to CDRUSNORTHCOM. As a subordinate unified command, SOCNORTH provides a

responsive and scalable capability to C2 SOF and conventional forces, when attached, in support of USNORTHCOM's mission. Commander, SOCNORTH, is the principal SOF advisor to CDRUSNORTHCOM. The SOCNORTH staff provides special operations expertise, advice, and assistance to USNORTHCOM, its Service components, and subordinate commands. SecDef assigns the TSOCs to US Special Operations Command under CDRUSSOCOM's COCOM and assigns OPCON of the TSOCs to the GCCs. SecDef also authorizes CDRUSSOCOM and the GCCs to establish support relationships when SOF commanders are required to simultaneously support multiple operations or commanders.

(g) **Joint Force Headquarters-National Capital Region (JFHQ-NCR).** JFHQ-NCR plans, coordinates, maintains situational awareness, and as directed, employs forces for HD and DSCA in the National Capital Region (NCR) joint operations area (JOA) to safeguard the nation's capital, excluding air defense and air warning. NORAD executes air defense operations within the USNORTHCOM AOR, to include the NCR, through the National Capital Region-Integrated Air Defense System (NCR-IADS).

(h) **United States Alaskan Command (ALCOM).** ALCOM is a subunified command under USNORTHCOM. The Commander, ALCOM, is assigned responsibility for HD and DSCA operations within the assigned ALCOM JOA by CDRUSNORTHCOM. ALCOM normally requires staff augmentation from the USNORTHCOM staff and Service components for HD and DSCA operations.

(i) **Joint Task Force-North (JTF-N).** JTF-N coordinates with DHS and other federal, state, and local drug law enforcement agencies (LEAs) to leverage military activities to support CT, counterdrug (CD), and counter transnational organized crime operations along US borders and littorals to disrupt transnational criminal organizations (TCOs) and deter their freedom of action in order to protect the homeland. JTF-N is an element of USNORTHCOM under OPCON of CDRUSARNORTH.

(j) **USNORTHCOM Contingency JTF(s).** When combat forces for a joint HD operation are attached to USNORTHCOM, CDRUSNORTHCOM exercises command authority delegated by SecDef, as necessary, to accomplish required missions or tasks. Based upon the scope and objectives of the operation, CDRUSNORTHCOM may decide to establish one or more subordinate JTFs. For example, Joint Task Force-National Capital Region, when activated, could have combat forces attached to conduct HD operations within its respective JOA. For various HD contingencies, CDRUSNORTHCOM may task a component command(s) or supporting commanders to provide the core of a new JTF HQ with augmentation from the other Service components.

(3) **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; the critical infrastructure of the US and its territories; and the domestic population and critical infrastructure of the sovereign nations, commonly called freely associated states, under the Compact of Free Association in the USPACOM AOR. The US territories located in the Pacific and the nations included in the Compact of Free Association include American Samoa; Northern

Mariana Islands; Guam; Baker, Howland, and Jarvis Islands; Johnston Atoll; Kingman Reef; Midway Atoll; Palmyra Atoll; Wake Atoll; the Federated States of Micronesia; the Republic of the Marshall Islands; and the Republic of Palau. USPACOM also contributes to the active, layered defense-in-depth of the western approaches to CONUS and Alaska. CDRUSPACOM is the supported commander for HD within the USPACOM AOR. Support relationships are coordinated among CCDRs with geographic HD responsibilities such as against threats from outside the AOR (e.g., USPACOM supporting USNORTHCOM). CDRUSPACOM may be tasked to support the collaborative federated architecture for targeting required by CDRUSNORTHCOM.

(a) **C2 for HD Land Operations in the USPACOM AOR.** Commanding General (CG), United States Army, Pacific Command (USARPAC), assumes functional component commander responsibilities as the land component commander for the USPACOM portion of the US and its territories. CG USARPAC is responsible for Joint Task Force-Homeland Defense (JTF-HD) to conduct operations within the USPACOM JOA (including CBRN response and DSCA) and for working closely with applicable federal, state, tribal, and local agencies when orchestrating DOD operations. All HD activities are coordinated with USNORTHCOM, USSTRATCOM, and others across AOR boundaries, including those concerning Hawaii and Alaska.

(b) **C2 for HD Maritime Operations in the USPACOM AOR.** The Commander, United States Pacific Fleet (COMUSPACFLT), conducts MHD operations in the USPACOM AOR, supports CDRUSNORTHCOM in the conduct of MHD operations in the USNORTHCOM AOR, and supports USCG MHS operations. COMUSPACFLT conducts MHD operations with assigned forces within the USNORTHCOM AOR in close coordination with USNORTHCOM's JFMCC while keeping CDRUSPACOM informed. Upon declaration of an MHD mission in the USPACOM AOR, the USCG allocates forces to CDRUSPACOM under the C2 of CGDEFOR West, which may be attached with specification of TACON to COMUSPACFLT, or OPCON if mutually agreed with the USCG. Figure II-2 depicts the applicable MHD and MHS command relationships.

(c) **C2 for HD Joint Air Operations in the USPACOM AOR.** The Commander, Pacific Air Forces (COMPACAF), is the theater JFACC for the USPACOM AOR and maintains a theater joint air operations center in Hawaii.

See JP 3-30, Command and Control of Joint Air Operations, *for details regarding theater JFACC, the joint air operations center, and C2 for joint air operations.*

(d) **C2 for HD Space Operations in the USPACOM AOR.** USSTRATCOM conducts space operations in direct support to USPACOM's HD operations. CDRUSSTRATCOM has designated JFCC Space as USSTRATCOM's SCA, responsible for the deconfliction, prioritization, and integration of military, intelligence, civil, and commercial space requirements between CDRUSSTRATCOM and CDRUSPACOM. CDRUSPACOM has designated COMPACAF as USPACOM's SCA to conduct joint space operations planning, to include ascertaining space requirements in support of USPACOM's HD operations. CDRUSPACOM or CDRUSSTRATCOM may authorize DIRLAUTH between the SCAs to ensure prompt and timely support.

(e) **C2 for HD CO in the USPACOM AOR.** CDRUSPACOM is responsible for defending against, mitigating, and defeating cyberspace threats against specific USPACOM systems that are not associated with the DODIN. HQ USPACOM will coordinate CO with USPACOM component commands, subordinate unified commands, JTFs, direct reporting units, and other CCMDs through USPACOM's CO support staff; USCYBERCOM provides a cyberspace forward support element to USPACOM to support CO and as required for liaison between USCYBERCOM and USPACOM components. For HD, USPACOM coordinates through USCYBERCOM with DHS through its CS&C as the primary agency for protecting USG and public networks against cyberspace intrusions and attacks. Functional CCDRs and the Services are responsible for protection of their networks located within the USPACOM AOR, but not assigned or attached to USPACOM.

(f) **C2 for HD Special Operations in the USPACOM AOR.** Special operations conducted in the USPACOM AOR are normally conducted with CDRUSPACOM as the supported commander while OPCON is exercised through the Special Operations Command Pacific (SOCPAC). In the USPACOM AOR, SOCPAC conducts TSOC functions and serves as the USPACOM entry point for all SOF matters. SOCPAC is tasked to conduct regional activities that may support future operations.

(g) Commander, JTF-HD, employs two task forces and subordinate coordination teams in two Pacific OAs (i.e., Task Force East in Hawaii and Task Force West in Guam). These forces, along with local installations, conduct HD operations and respond to support requests from civil authorities per USPACOM CONPLAN 5001-13, *Defense Support of Civil Authorities (DSCA).*

(h) To assist Commander, JTF-HD, in accomplishing HD missions, organizations such as the USPACOM Joint Intelligence Operations Center (JIOC), Joint Interagency Task Force-West (JIATF-W), SOCPAC, and USPACOM Service components provide intelligence, staff augmentation, interagency coordination, and military forces as necessary. The USPACOM JIOC provides support to the Federal Bureau of Investigation's (FBI's) Honolulu Joint Terrorism Task Force (JTTF), with an analyst imbedded as a member of the DOD analytical team residing within the Honolulu JTTF. All USPACOM Service and functional components involved in HD operations provide situational awareness and coordinate their actions with JTF-HD, per USPACOM CONPLAN 5002, *Homeland Defense.*

(4) **Commander, United States Southern Command (CDRUSSOUTHCOM).** CDRUSSOUTHCOM provides contingency planning, operations, and security cooperation for Central and South America, the Caribbean (except US commonwealths and territories and foreign nations and territories within the USNORTHCOM AOR), and Cuba, as well as for the FP of US military resources within these locations. CDRUSSOUTHCOM is also responsible for defense of the Panama Canal and canal area. Key contributions to defending the homeland are to provide:

(a) Interdiction of air and maritime threats to the homeland before they enter the USNORTHCOM AOR and C2 military handoff when/as appropriate.

(b) Designated lead CCDR element within Joint Interagency Task Force-South (JIATF-S). JIATF-S works with PNs and US LEAs to stem illegal production and trafficking of illicit drugs and precursors and to counter the affiliated TCOs, which undermine the security of nations in the USSOUTHCOM and USNORTHCOM AORs and threaten overall US national security. USSOUTHCOM's role provides significant insight into extant and emerging threats to the homeland. This includes contacts established during JIATF-S missions that may be determined by USSOUTHCOM or USNORTHCOM to be an HD threat.

(5) **Commander, United States European Command (CDRUSEUCOM); Commander, United States Africa Command (CDRUSAFRICOM); and Commander, United States Central Command (CDRUSCENTCOM).** CDRUSEUCOM, CDRUSAFRICOM, and CDRUSCENTCOM play vital roles in defending the homeland and supporting CDRUSNORTHCOM and CDRUSPACOM for HD. Specifically, they provide a forward presence to obtain information on threats that may be planning attacks on the homeland, and they can deny adversaries freedom of access to the air, land, and maritime approaches to the homeland. CDRUSEUCOM and CDRUSCENTCOM may be tasked to support the collaborative federated architecture for targeting required by CDRUSNORTHCOM.

c. **Functional CCDR Responsibilities**

(1) **CDRUSSTRATCOM.** CDRUSSTRATCOM is the lead CCDR for strategic deterrence planning and executes strategic deterrence operations, as directed. Specifically, CDRUSSTRATCOM conducts the following activities associated with defending the homeland:

(a) Synchronize planning for global missile defense and coordinate global missile defense operations support. Provide missile warning information to CCDRs and allies, and assessment of missile attack if the appropriate CCMD is unable to do so. Provide alternate global missile defense execution capability as directed and, as required, to ensure COOP.

(b) Plan, coordinate, and execute nuclear, conventional, or global strike, as directed.

(c) Support the collaborative federated architecture for targeting required by CDRUSNORTHCOM for HD.

(2) USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities for offensive cyberspace operations (OCO), DCO, and DODIN operations and conducts CO to enable actions in the physical domains, facilitates freedom of action in cyberspace, and denies the same to adversaries. USCYBERCOM can support HD CO in collaboration with USNORTHCOM, USPACOM, and DHS by coordinating activities within the required AOR and assisting with expertise and capabilities directed and made available.

(a) USCYBERCOM synchronizes planning for CO, to include direction of DODIN operations and defense to secure, operate, and defend DOD cyberspace and to defend US critical cyberspace assets, systems, and functions. Directs DODIN operations and defense in coordination with the CJCS and CCMDs. Coordinates with other CCMDs and appropriate USG departments and agencies prior to the creation of cyberspace effects that cross AORs in response to cyberspace threats.

(b) USCYBERCOM normally provides cyberspace forward support elements to CCMDs to support CO during major operations and exercises and for liaison between the GCCs' components and USCYBERCOM Service components, as required.

For details regarding USCYBERCOM and all aspects of CO, see JP 3-12, Cyberspace Operations.

(3) **CDRUSSOCOM.** CDRUSSOCOM leads, plans, synchronizes, and, as directed, executes global operations against terrorist networks. US Special Operations Command also organizes, trains, equips, and deploys combat-ready SOF in support of other CCMDs, while retaining COCOM of the TSOCs. For operations conducted in the homeland, CDRUSSOCOM serves as either a supported or supporting commander for selected CT activities and serves as a supporting commander to the GCCs with geographic HD responsibilities within their respective AORs. USSOCOM also integrates planning for DOD countering weapons of mass destruction (CWMD) efforts. This CWMD effort is directly coordinated, synchronized, and integrated with the Defense Threat Reduction Agency (DTRA), CCMDs, USG departments and agencies, international organizations, NGOs, and foreign partners. USSOCOM integrates and synchronizes DOD-wide efforts in support of the CWMD mission by planning, advocating, and advising CCMDs on WMD-related matters, to include doctrine, organization, training, materiel, leadership, education, personnel, and facilities.

(4) **CDRUSTRANSCOM.** CDRUSTRANSCOM provides common-user and commercial air, land, and sea transportation; terminal management; patient movement; and aerial refueling to supported commanders. For HD operations, CDRUSTRANSCOM provides, upon request, a director of mobility forces to advise on air mobility support operations.

d. **Reserve Component (RC) Responsibilities.** The RC of the US Armed Forces consists of the ARNG, the Army Reserve, the Navy Reserve, the Marine Corps Reserve, the ANG, the Air Force Reserve, and the USCG Reserve. By virtue of their geographic dispersion throughout the US, the RC represents a significant military response capability for HD missions and activities.

e. **NG.** The NG is forward-based in nearly 3,000 communities throughout the US; the territories of Guam, the US Virgin Islands, and Puerto Rico; and the District of Columbia. It is readily available to conduct domestic operations, including HD, DSCA, NG civil support, and HS activities. As a military organization, the NG routinely interacts with state and local emergency managers; local LE; first responders; and Title 10, USC, forces. The NG is experienced in supporting neighboring communities in times of crisis. NG forces

have both federal and state responsibilities specified in the Constitution of the US; Title 10, USC; Title 32, USC; and applicable state constitutional provisions and statutes. It operates not only as RCs of the USA and the USAF supporting the President and their assigned CCMDs when under Titles 10 and/or Title 32, USC, in time of war and in national contingencies, but also as an organized militia supporting governors in domestic operations in Title 32, USC, or state active duty status. It is important that other Service/component commanders and staffs understand that the statutory roles and authorities of NG forces, when acting under state control, vary from state to state. Governors may employ the NG for the HD mission in state active duty status or as provided in Title 32, USC, Section 902, when approved by SecDef, for HD activities such as critical infrastructure protection (CIP). When federalized pursuant to Title 10, USC, NG units and personnel are subject to federal C2.

For more detailed information regarding the NG and HD, see DODD 3160.01, Homeland Defense Activities Conducted by the National Guard.

(1) **NGB.** NGB is a joint activity of DOD and serves as the channel of communications for all matters pertaining to the NG between the Departments of the Army and Air Force, the 50 states, District of Columbia, Commonwealth of Puerto Rico, Guam, and the US Virgin Islands. CNGB is the principal advisor to SecDef, through the CJCS, on matters involving non-federalized NG forces and on NG matters to the Secretaries of the Army and Air Force and to the Service chiefs of the Army and Air Force. The NGB participates with the USA and USAF staffs in the development and coordination of programs pertaining to or affecting the NG. The NGB formulates and administers the programs for the training, development, and maintenance of the ARNG and ANG.

(2) **The Adjutants General (TAGs).** The non-federalized NG is commanded and controlled by the governor through TAG of each state (or, in the case of the District of Columbia, by SecDef through the CG of the District of Columbia NG). TAG exercises C2 through their applicable National Guard Joint Force Headquarters-state (NG JFHQ-State).

For more information on the roles and responsibilities of TAGs, see DODD 5105.83, National Guard Joint Force Headquarters-State (NG JFHQs-State).

(3) **Reserves.** The reserves, at all times, are subject to a federal chain of command pursuant to Title 10, USC, as defined by their parent Service. The USCG Reserve is subject to both Title 10, USC, and Title 14, USC, under the direction of the Commandant of the USCG.

For additional information on the RC mobilization/demobilization process, see JP 4-05, Joint Mobilization Planning.

e. **CCDRs HD Relationships.** 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. In consideration of strategic direction, the JFC establishes the priorities, timelines, goals, and objectives for HD missions that allow synchronization and integration of all operations for

unified action. Federal and international law, international and command agreements, DOD policies, and selected plans provide guidance which the CCDR must integrate to achieve synchronization. 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 in order to enhance coordination for planning and execution of cross-AOR operations. CAAs must remain consistent with DOD guidance as promulgated from SecDef and the CJCS. The CAA between CDRUSNORTHCOM and CDRUSPACOM establishes the methodology under which transfer of forces between the two CCMDs is executed in support of HD missions. Additionally, per DOD policies, CNGB and the state NG forces must be coordinated and synchronized within both the planning and execution phases to ensure unity of effort. Processes, C2 arrangements, and communication requirements are representative items addressed in the document.

4. Interagency Coordination

a. **Interorganizational Coordination and Interoperability.** During an HD operation, civil authorities may span the gamut of being fully functional to non-existent, or could contain any combination of federal, state, and local authorities. The events that initiate an HD operation are so diverse, it is difficult to estimate the civilian functions likely to be functional and can only be determined as the situation develops. HS activities of some interorganizational partners may overlap with some HD activities, and while the major military activities that are the responsibilities of DOD cannot be accomplished by other interorganizational partners, their support is essential. Unity of effort among all HD participants is fundamental and essential. HD operations are conducted in a complex OE that contains thousands of different jurisdictions (federal, state, tribal, and local), many agencies and organizations, the private sector, and several allies and multinational partners. From a USG perspective, this necessitates coordinated and integrated activities that have been previously exercised/rehearsed to facilitate effective interagency interoperability in addition to unity of effort. Coordination should be conducted through the defense coordinating officer/defense coordinating element (DCE) of the affected region. The inherent interrelationships between HS, HD, and DSCA, and the potential for transition between those missions, creates a dynamic and complex environment in which interorganizational coordination and resulting interoperability could prove critical. From a DOD perspective, understanding and executing the multiple command relationships and organizational relationships required for simultaneous execution of HS, HD, and DSCA requires the utmost in interagency coordination.

(1) Within the US homeland and its approaches, forces may face continuous media scrutiny. When faced with media questions or scrutiny, consult with the public affairs (PA) office before responding. This is due to the sensitive jurisdictional considerations and political dimensions of a domestic response.

(2) Operational coordination is conducted within appropriate joint force command centers and their corresponding non-DOD counterparts. It is not complete until

it includes interorganizational planning considerations, which are intrinsic rather than optional in the planning process. CDRUSNORTHCOM and/or CDRUSPACOM may seek approval and guidance from SecDef to conduct interorganizational planning and coordination when appropriate.

(3) Each CCDR has the prerogative to organize or tailor the interorganizational coordination function differently based on mission requirements. Regardless of the title of the interorganizational coordination effort, it should include agency representatives, command liaison officers (LNOs), and staff representatives who collaborate to share information; analyze ongoing activities, actions, implications, and/or consequences; and participate in planning. Interorganizational coordination efforts should ensure the commander and staff are completely informed on interagency issues and implications.

For more information on interagency coordination, refer to JP 3-08, Interorganizational Cooperation.

(4) Information sharing is critical to the efficient pursuit of unity of effort. A proven approach to information sharing during interorganizational cooperation is the use of transparency to develop shared situational awareness of common objectives. Commanders and interorganizational partners should provide guidance on what information needs to be shared with whom, when, and how. DOD's over-reliance on the classified information system for both classified and unclassified information is a frequent impediment, and the means of sharing the information must be established in advance. DOD information should be appropriately secured, shared, and made available throughout the information life cycle to appropriate mission partners to the maximum extent allowed by US laws and DOD policy. Critical to transparency of information sharing is the proper classification of intelligence and information.

b. **MHD and MHS Coordination.** MHD and MHS are closely related, but separate activities based on the distinct authorities used to implement either MHD or MHS tasks. The Title 14, USC, functions and powers of the USCG enable USCG commanders to conduct a broad spectrum of regulatory functions and MHS activities, while maintaining the capability and readiness to rapidly transition to execute Title 10, USC, MHD tasking when required. USCG regulatory functions, such as captain of the port (COTP) authorities and marine transportation system/waterways management activities, may be used to support or complement MHD operations. MHS activities and USCG regulatory functions are not conducted under CGDEFOR C2 due to the limitations of Title 10, USC, authority. JFCs seeking to leverage USCG regulatory functions or MHS activities must coordinate with the appropriate USCG area commander. DOD forces that are provided to support MHS operations are TACON to specifically designated USCG commanders. Figure II-2 depicts the C2 of both MHD tasks pertaining to CGDEFOR, as discussed in applicable EXORDs and interdepartmental agreements, and MHS tasks that are conducted under USCG-specific authorities.

For more information on coordination of USCG-specific authorities, see JP 3-08, Interorganizational Cooperation.

(1) **MHD Tasks.** MHD tasks conducted under the C2 of DOD forces are categorized under the joint functions and are subject to SROE (see Chapter III, "Planning and Operations for Homeland Defense").

(2) **MHS Tasks.** MHS tasks and related regulatory functions are conducted under the C2 of USCG commanders, are further described in USCG policy directives and doctrine, and are subject to USCG use of force policy. Certain MHS tasks may require immediate USCG access to DOD capabilities and forces. CDRUSNORTHCOM, CDRUSPACOM, and CDRUSSOUTHCOM may transfer forces to operate under the TACON of USCG commanders for MHS operations upon request by the USCG. In certain circumstances, SecDef authorization may be required to reallocate forces or approve a request for assistance to support MHS for 48 hours or more. DOD forces conducting MHS operations under USCG C2 must adhere to USCG use of force policy for warning shots and disabling fire.

For more information on MHS tasks and USCG use of force policy, see Commandant Instruction (COMDTINST) M16600.6, Maritime Security and Response Operations (MSRO) Manual; *COMDTINST M16247.1,* Maritime Law Enforcement Manual (MLEM); *COMDTINST M16600.3,* Underwater Port Security Operations Manual; *and Coast Guard Publication 3-0,* Operations.

For more information on USCG regulatory functions concerning ports and waterways, see COMDTINST M16000.11, Marine Safety Manual, *Volume VI,* Ports and Waterways Activities.

For more information on the force transfer process for DOD support to MHS operations, see the CJCS MHD EXORD, CJCS DSCA EXORD, and 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.

c. **MOTR Process**

(1) The MOTR Plan aligns the response to maritime threats against the US. The MOTR Plan has been used to facilitate the resolution of many maritime threat responses ranging from migrant interdictions and drug seizures to terrorism and piracy. Operational protocols complement the plan with detailed guidance for specific types of cases and agency/department contact information.

(2) The MOTR Plan provides the framework for integrated military, LE, diplomatic, and intelligence community (IC) action. Ensuring an aligned response is particularly challenging in the maritime environment where multiple USG departments and agencies may be involved, each having separate authorities, responsibilities, and capabilities.

(3) The MOTR Plan supports, for example, the coordinated response to a vessel suspected of illicit trafficking. Such a response may include identifying the legal basis for boarding, enactment of diplomatic efforts with a vessel's flag state, and resolution of

investigative and disposition determinations, all of which potentially involve multiple USG departments' and agencies' authority and jurisdiction.

(4) The Global MOTR Coordination Center facilitates the coordination process and serves as the executive secretariat for implementation of the MOTR Plan. During MOTR coordination activities, the Global MOTR Coordination Center is accountable to the NSC staff (see National Security Presidential Directive [NSPD]-41/Homeland Security Presidential Directive [HSPD]-13, *Maritime Security Policy*).

(5) Successful MOTR execution relies on the operations-intelligence linkage enhanced by ongoing efforts to achieve maritime domain awareness and to facilitate timely decision making. The objective is to identify threats as early and as distant from the homeland as possible, but no later than the time required to defeat or otherwise overcome threats at a safe distance from the US. This is enabled by maritime domain awareness.

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

d. **Land Operational Threat Response**

(1) The homeland is a unique theater of operations for US ground forces and is subject to special requirements. The USA and USMC components to USNORTHCOM and USPACOM work with DHS, other interagency partners, and civil authorities to support HS, which complements some aspects of HD. The USA and USARNORTH also support security cooperation activities with North American partners to help build a cooperative military defense as part of the effort to secure the land approaches and ensure defense of the homeland in-depth.

(2) Many of the missions and activities that are conducted by the land component during shaping operations support other interagency partners and civil authorities, (e.g. defense support of LEAs, CD, CWMD, countering TCOs, FP, security cooperation activities with Mexico and The Bahamas, and partnership with Canada). These efforts contribute to, and are enablers to, both HS and HD. Those efforts help constitute the prevent aspect of HD. The sharing of identity information between interagency partners is a key enabler to manage and track cross-border movement. NSPD-59/HSPD-24, *Biometrics for Identification and Screening to Enhance National Security,* instructs all federal agencies to make available to other agencies biometric and associated biographical and contextual information associated with persons of interest. Operational commanders collect and provide identity information on terrorists encountered in the OE to the NCTC through the Defense Intelligence Agency (DIA) Watch Listing Division.

For additional information on joint land operations, refer to JP 3-31, Command and Control for Joint Land Operations.

e. **AOTR Process**

(1) An AOTR ensures a comprehensive and coordinated USG response to air threats against the US or its interests. NSPD-47/HSPD-16, *Aviation Security Policy,*

prescribes the AOTR Plan as part of the overall national aviation policy. Simply stated, the AOTR is primarily to counter asymmetric threats involving civilian aviation, but includes considerations for interagency coordination to defend against foreign military air and missile attacks. Several DOD HD responsibilities fall within the protocols of the AOTR. DOD response capabilities remain an integral part of the overall national response in support of HD and HS complementary objectives and missions.

(2) AOTR comprises immediate actions, generally short duration in nature, to counter the full range of airborne and ground-based aviation security threats. These threats include, but are not limited to: attacks using civilian aviation (i.e., commercial/general aviation) manned and unmanned aircraft as weapons against ground-based or airborne targets; attacks against aircraft, including hijacking and air piracy; attacks using standoff weapons, including man-portable air defense systems; attacks involving civilian aircraft carrying WMD; and attacks against aviation transportation system infrastructure. AOTR execution begins when intelligence or other information is received that an incident is imminent or occurring and that an immediate response is necessary and concludes when the threat has been defeated or otherwise resolved.

(3) Upon AOTR execution and time permitting, DOD initiates secure communications with appropriate departments and agencies to facilitate the timely flow of information. This will allow for appropriate consultation related to the initial DOD airborne operational response, as well as coordination of related LE actions or other security measures. DOD performs the following activities specific to AOTR, as appropriate:

(a) Specific Airborne Threats (an ongoing or potential attack from the air):

1. Through CCDRs and NORAD, SecDef directs the necessary supporting measures to facilitate effective response and to mitigate subsequent effects of an ongoing or potential attack from the air. In extreme circumstances, this includes a determination, made in consultation with the Department of Transportation (DOT) and DHS, whether to implement emergency security control of air traffic measures. Unless the President directs otherwise, DOD is the only USG department authorized to direct engagement using deadly force against airborne civilian aircraft that present an imminent threat to the US or US interests.

2. Interception of designated flights of interest that do not present an immediate threat to the US or its interests, as deemed necessary by SecDef or designee. This includes response to a threat against aircraft with US persons onboard that occurs overseas, in coordination with the Department of State (DOS) and the affected countries, as appropriate.

3. Conducting air defense against airborne hostile military threats.

(b) General Threats:

1. Conducting air defense against threats to DOD assets and infrastructure on DOD installations.

2. Response to other aviation threats globally, including airborne or ground-based actions taken at the request of foreign partners and when directed by SecDef or the President.

For more information on the full range of air operations, refer to JP 3-01, Countering Air and Missile Threats, *and JP 3-30,* Command and Control of Joint Air Operations. *For more information on the AOTR, refer to the* Aviation Operational Threat Response Plan.

5. Interorganizational Cooperation Considerations

a. The threat exists across a continuum that ranges from nation states down to individuals and small groups, who are intent on doing harm to the US. Today, HD mission response forces involve multiple organizations. Operation NOBLE EAGLE (ONE), the NORAD, USNORTHCOM, and USPACOM operation aimed at defending the homeland, involves active duty personnel from the USAF, USN, Canadian Forces, and NG members federalized for the mission. These military forces coordinate with DOT (FAA), DHS, the Department of Justice (DOJ), and other USG departments and agencies, as appropriate. A response to a possible hijack situation would involve the private sector as well as local first responders. For example, airline companies, private or municipal airports, local municipalities, and other non-federal entities are responsible for the aircraft and any airports where the aircraft may attempt to land or be directed to land. This demonstrates the complex environment in which DOD forces must respond to threats that involve multiple jurisdictions (federal, state, territorial, local, and tribal) with domestic partners and international/multinational partners (e.g., NORAD).

b. The HD C2 structure will depend upon early identification of the responsibilities, authorities, and capabilities of USG organizations which support HD, plus the additional considerations of other governmental organizations or NGOs, and multinational forces. The resulting complexity of C2, mission planning, and operational execution should drive early identification of the desired end states and necessary collaboration with the operational partners. Moreover, the JFC with HD missions should also account for likely media scrutiny and sovereignty and jurisdictional issues. For example, MHD operations may transition from HD to HS to DSCA missions, or vice versa, with the selection of the primary agency being dependent upon both the developing real-time situation and the USG desired end state. HD, HS, and DSCA operations can occur simultaneously or transition from one to another. HD missions in the homeland and in the approaches are truly dynamic as situations may change in minutes or hours versus days or weeks.

For additional information on interorganizational cooperation, refer to JP 3-08, Interorganizational Cooperation.

6. Multinational Forces

To conduct the full range of HD operations, CCDRs should consider multinational and nonmilitary organizations. When a response force resides within an alliance, the procedures and structure of that alliance will normally determine the operational-level leadership. When a response force is based in a coalition (or a lead-nation structure in an

alliance), the designated lead nation or other leadership mechanism will normally select the operational-level leadership. While the President and SecDef retain command authority over US forces, it is often prudent or advantageous to place appropriate US forces under the TACON of a foreign commander for reasons such as maximizing military effectiveness and ensuring unity of effort.

a. **Security Cooperation Efforts.** The US seeks the cooperation of numerous foreign governments, multinational forces, and other international partners to achieve its national security goals, to include defense of the homeland. CCDRs integrate this cooperation with their theater campaign plans (TCPs) and conduct security cooperation activities to encourage and enable countries to work with the US to achieve strategic objectives. Strengthening security relations with multinational partners increases their capabilities to contend with common challenges.

(1) In the forward regions, CCDRs and their components conduct security cooperation activities with PNs that help provide the outer layer of HD.

(2) GCCs with geographic HD responsibilities have AORs with very different characteristics. In addition to its vast airspace, the USPACOM AOR is predominantly maritime and includes considerable political, religious, cultural, social, and economic diversity. It encompasses the Asia-Pacific region, with numerous sovereign nations and one-half of the Earth's surface. The area includes five of seven US security treaty alliances and extensive international waters covered by international law, as well as US territories under US law, treaties, or compacts. The USNORTHCOM AOR is primarily continental, with extensive land borders and coastal regions. It includes Canada, Mexico, The Bahamas, Turks and Caicos Islands, Bermuda, the British Virgin Islands, Puerto Rico, the US Virgin Islands, and the US (excluding Hawaii and Pacific territories) with multiple legal and policy concerns. USNORTHCOM security cooperation efforts with Canada and Mexico directly impact US defense-in-depth.

(a) **Military Engagement and Shaping.** Security cooperation enhances access, readiness, and training by strengthening partnerships and regional security. This involves specific focus areas as described in the *Guidance for Employment of the Force* (GEF). GCCs with geographic HD responsibilities address commander's communication synchronization in their security cooperation planning efforts. CCDRs seek to diminish the conditions that terrorists exploit and to support activities that deny sanctuary to terrorists. The plans also strengthen and improve collaboration among joint commands, agencies at all levels of government, and regional partners.

(b) **Enabling Continental Defense.** Cooperative defense, in association with US regional partners, enhances successful continental defense, achieving collective security interests and the desired HS and HD shaping objectives established in the GCC's TCP. Security cooperation activities are essential to both USNORTHCOM support of HS and the HD mission through mutually beneficial partnerships. Military and civilian interoperability and cooperation begins by establishing and maintaining relationships. These relationships build to include combined education, training, military engagement, equipping, and exercises supported by intelligence and information sharing, exchange of

LNOs, and other activities that facilitate HD. Cooperative defense helps foster appropriate relationships to leverage complementary capabilities and capitalize on limited resources. Finally, current efforts toward an integrated North American defense warrant an increase in HD exercises and personnel exchanges.

(3) Various initiatives and agreements exist that forge relationships and provide for multinational coordination in the defense of the homeland. For example, the Canada-United States Combined Defense Plan is another step towards an integrated North American defense.

b. **Alliance Support to HD.** Various alliances may be a source of additional HD support. For example, Article 5 of the North Atlantic Treaty states: "… an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence…." When the US was attacked on 11 September 2001, the North Atlantic Treaty Organization (NATO) invoked Article 5 and provided NATO Airborne Warning and Control System aircraft to help patrol US airspace and initiated Operation ACTIVE ENDEAVOUR as part of an AT effort.

c. **Other Multinational Considerations.** Many activities can increase US partners' capabilities and create the conditions for establishing new multinational partnerships to contend with mutual challenges. The GEF outlines a series of security activities a CCDR can use to advance long-term security objectives with multinational partners wherever feasible and collectively supportive. These activities include:

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

(2) Counternarcotics assistance.

(3) CWMD activities.

(4) Defense and military contacts.

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

(6) Security force assistance, to include DOS security assistance programs.

(7) Forensics and biometrics capability and capacity building.

(8) Other programs and activities (e.g., Regional Defense Counterterrorism Fellowship Program and Defense Environmental International Cooperation).

(9) DOD SPP.

d. The OE and the coordinated and integrated action of all contributors may blur the distinct 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 organization has unique capabilities that may not be easily duplicated by other departments, agencies, or organizations. The supported JFC should continually address the challenge of coordinating, integrating, and synchronizing the wide range of available capabilities to defend the homeland. Employment of nonlethal capabilities should be considered in any situation requiring direct fire capabilities.

e. To achieve the objectives, unified action, and the synchronization and integration of military operations in time, space, and purpose, the JFC must consider many factors, to include:

(1) What objectives, when achieved, will 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 interorganizational 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?

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

CHAPTER III
PLANNING AND OPERATIONS FOR HOMELAND DEFENSE

1. General

The threat to the homeland is both difficult to predict and increasingly diverse. The likelihood of conventional large-scale land attack on the US may be remote. However, the wide range of threats that does exist must be addressed. In modern times, US forces have concentrated on defeating threats as far away from the homeland as possible and that remains the objective. The central idea is to protect the homeland from external threats and aggression using integrated strategic, operational, and tactical offensive and defensive measures as necessary. The ability to detect, deter, prevent, or, if necessary, defeat threats is a required capability to protect the homeland. Specific planning factors, requirements, and objectives for HD operations are contained in OPLANs and CONPLANs associated with the mission.

2. Strategic Guidance

General strategy is provided in high-level policy documents such as the *National Security Strategy* (NSS), *Defense Strategy Review,* and the NMS. Similarly, high-level planning guidance is provided in the UCP; GEF and CJCSI 3110.01, *(U) Joint Strategic Capabilities Plan (JSCP).* Planning architecture is provided in Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3130.03, *Adaptive Planning and Execution (APEX) Formats and Guidance.*

3. Operational Factors

a. **Civil and Military Relationships.** Civil-military relationships may be more complicated during HD operations because the military operations will be taking place in our homeland. Regardless of the size and scope of the particular operations, inevitably they will involve multiple jurisdictions (such as cities, counties, regions, tribes, and states). As a result, multiple agencies and organizations will participate. Some may directly or indirectly support military operations and some may conflict with them, not because of different loyalties, but because of different authorities. Managing such relationships will require significant time and effort on the part of federal, state, local, and tribal authorities to ensure proper coordination. Interagency forums, associations, information sharing, and constant communications will be vital enablers. Interorganzational coordination and synchronization with governmental and nongovernmental entities, as well as ensuring conformity with the Response Federal Interagency Operational Plan, may assume a level of importance not matched in most overseas theaters of operations.

For additional information on civil and military relationships during a domestic incident, see PPD-25, Guideline for US Government Interagency Response to Terrorist Threats or Incidents in the US and Overseas.

b. **Commander's Communication Synchronization and PA**

(1) CJCSM 3130.03, *Adaptive Planning and Execution (APEX) Formats and Guidance,* requires the JFC to include communication goals and objectives in the commander's intent and to have a communication approach that ensures unity of themes, objectives, and messages among key activities; consistency in intent or effect between command operations, actions, and information; and a risk assessment of the information that may reach unintended audiences, create unintended consequences, and require risk mitigation measures.

For more information, see JP 3-0, Joint Operations; *JP 3-61,* Public Affairs; *and JDN 2-13,* Commander's Communication Synchronization.

(2) **PA.** The role of PA in HD operations is to support the JFC by communicating truthful and factual unclassified information about DOD activities to US, allied, national, and international audiences, publics, and stakeholders. Due to the involvement of other USG departments and agencies in HD missions, PA will require interagency cooperation, coordination, and unity of effort. PA in HD operations enables all USG departments and agencies to speak with one voice and provide consistent, factual information to the public. As the LFA for HD, DOD develops key messages and provides PA guidance. Supporting agencies conduct their respective PA operations in concert with this guidance. PA should be included in all phases of planning and coordination from the onset of HD operations. Specific DOD PA responsibilities are outlined in various CCMD plans and standing PA guidance. The EXORD for the incident will provide the PA posture and media engagement policy. Incident-specific guidance will be developed by the primary agency in coordination with participating agencies.

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

c. **Non-DOD Federal, State, Territorial, Local, and Tribal Planning Factors**

(1) Interorganizational cooperation must occur between elements of DOD and non-DOD federal, state, local, and tribal agencies, as well as other participating USG departments and agencies for the purpose of achieving HD objectives. Commanders of USNORTHCOM and USPACOM have designated DCEs assigned to each of the 10 respective Federal Emergency Management Agency (FEMA) regions. Each Service has state EPLOs assigned to the same regions designated to conduct interagency coordination. Service EPLOs usually coordinate with NG JFHQs-State joint operation centers. Each FEMA region also contains additional NG planners to assist CCMD planners. Positive and active participation by command interagency staff members from the interagency coordination office, group, or planning cell can be used to mutual benefit.

(2) Commanders and their staffs should consider the interrelationship between HD and DSCA operations (i.e., the potential for transition between the missions and simultaneous operations).

d. **Legal Considerations.** Military operations inside the homeland can present unique and complex legal issues. Certain military functions (e.g., intelligence operations, ROE, and RUF) have specific applications and legal implications when conducted

domestically. Coordination with the servicing office of the staff judge advocate for legal advice should be as early in the operation planning process as possible.

4. Intelligence Sharing for Homeland Defense

a. The success of interorganizational cooperation in HD operations hinges upon timely and accurate information and intelligence. Information sharing environments should include as many essential participants as possible, understanding that not all are capable of participating in a collaborative environment. When possible, a collaborative intelligence sharing environment should be capable of generating and moving intelligence, operational information, and orders where needed in the shortest possible time. Intelligence staff responsibilities can be found in the JP 2-0 series. Coordination for information sharing, and especially intelligence sharing, should begin early in all HD planning processes.

b. The architecture which supports this type of environment needs to be dynamic, flexible, and capable of providing multinational partners and interagency participants rapid access to appropriate data. It should facilitate the capability of the IC to support the JFC and subordinate joint force components and to integrate support from and to non-DOD agencies and NGOs as needed.

c. The intelligence sharing architecture is configured to provide the baseline data needed to support commanders at all levels. CCDRs are responsible for the intelligence sharing architecture for their commands and all assigned, attached, and supporting elements. For contingency operations, subordinate JFCs, supported by their intelligence directorates, are responsible for establishing the intelligence architecture required to accomplish the HD mission. In HD, it is particularly important that effective fusion of intelligence, counterintelligence (CI), LE information, and other available threat information occurs. This will assist in developing a more accurate assessment of threats to the homeland and may prevent surprise.

d. The parameters under which DOD operates are different in the US than they are overseas. In the past, one individual typically dealt with foreign information and the other domestic. Today both involve elements of foreign and domestic information. Determining the nature of the data required and the right units to gather it are areas that often require judge advocate input regarding the legal authorities for information gathering. Intelligence activities in the homeland are strictly governed by the Constitution; applicable laws; the policies and procedures authorized in DODD 5240.01, *DOD Intelligence Activities;* and other relevant DOD policies (e.g., intelligence oversight). These policies permit DOD intelligence missions in the homeland if the subject of the intelligence effort is definitively linked to defense-related foreign intelligence and CI activities. Intelligence oversight policies also provide established guidance and requirements to perform activities or missions not intelligence related (e.g., using domestic imagery for incident assessment and awareness). However, intelligence oversight policies also provide specific guidance and regulations to ensure or safeguard against unauthorized collection against US persons (citizens, legal residents, and organizations). Special emphasis shall be given to the protection of the Constitutional and privacy rights of US persons.

e. LE information received by DOD frequently contains US person information. US person information or information concerning persons and organizations not affiliated with DOD is subject to various statutory and regulatory rules and processes. Military criminal investigation organizations' agents or the FBI may provide sensitive threat information derived from ongoing LE or CI investigations. It is imperative DOD personnel handling LE information be fully cognizant of all restrictions and processes for receipt, retention, handling, dissemination, and oversight.

f. Intelligence activities specific to the NG are covered by CNGB Instruction 2000.01 series, *National Guard Intelligence Activities,* and CNGB Manual 2000.01, *National Guard Intelligence Activities.*

5. Joint Fires

Joint fires are fires delivered during the employment of forces from two or more components in coordinated action to produce desired effects in support of a common objective. Joint fires may be provided to assist air, land, maritime, or special operations forces in conducting HD activities within an OE framed by complex legal authorities and significant interagency coordination. Although major operations against an enemy in the US remain highly unlikely, various threats require capabilities and preparations to deter or defeat them. For that reason, the supported JFCs for HD have plans/orders for HD operations that anticipate the use of joint fires across the range of military operations. The following preparations provide useful examples of the challenges of employing joint fires in HD.

a. **Deterrence and Preemptive Self-Defense.** The complexity and diversity of the strategic threats to the homeland range from intercontinental ballistic missiles (ICBMs) to terrorists with WMD. The common factor is that such attacks would have a devastating effect of strategic proportions. From a joint fires perspective, HD capabilities have a deterrent effect that minimizes the threat of an overt attack of strategic proportion by an enemy. For threats from rogue states and non-state actors, deterrence may not work, so an active, layered defense-in-depth complements the deterrence capabilities. Also, the use of joint fires, to include global strike options in preemptive self-defense, is a strategic consideration.

(1) The threat of ballistic missile attack against the homeland is the one strategic threat that would require the use of fires to protect the homeland. The limited defense option for BMD is discussed under paragraph 7, "Protection."

(2) ONE. While initially conceived in the immediate aftermath of the 11 September 2001 attacks, this operation incorporates both the response to terrorist use of aircraft as weapons and NORAD's air defense mission. ONE and air defense is discussed under paragraph 7, "Protection."

(3) Terrorist threats to the homeland from overseas may require use of joint fires through military CT operations or in support of LE activities. Terrorist threats within the

homeland are an HS mission rather than a matter of HD, unless directed otherwise by the President.

b. **Maritime Joint Fires.** Maritime joint fires provide significant capabilities against any maritime-based threat to the homeland. The maritime environment, including the sea approaches to the homeland, may afford opportunities to employ joint fires in support of both HS and HD. Maritime forces can be employed to rapidly destroy, intercept, or neutralize conventional and terrorist threats, both at sea and ashore. These assets are used to keep potential threats at bay, far from US shores, but could be deployed close to home if threats dictate. Use of fires for lethal or nonlethal effects are options. The maritime aspect of air and missile defenses are discussed under paragraph 7, "Protection."

(1) A variety of maritime threats to the homeland exists and may include cargo ships, fishing boats, semi-submersibles, and military vessels. Once a vessel has been identified as a threat to the homeland, maritime forces' options may be employed to detect, deter, prevent, and defeat the delivery of the weapons, cargo, or people to the intended target(s). Maritime forces may take action as defined by the chain of command, the SROE and supplementary measures, if any.

(2) Depending on the threat, MHD options may be determined through the MOTR Plan protocol process. Within the USNORTHCOM AOR, the JFMCC directs MHD operations that may include appropriate Service or SOF assets to detect, deter, prevent, and defeat threat vessels.

c. **Land-Based Fires.** HD presents complex operational challenges for joint fires due to the necessity to achieve unity of effort within an OE of sovereign states (with NG units) and the need to interface with a number of disparate government agencies, NGOs, and the private sector. Land-based fires for HD operations require interorganizational cooperation, especially since there is significant overlap between DOD executing HD and LE organizations executing HS and supporting HD. Land-based fires for air and missile defenses are discussed under paragraph 7, "Protection."

d. **Supporting Fires.** Conducting HD, US-only air missions may require a high degree of dynamic targeting that relies on rapid coordination and integration of assessment, surveillance, and attack assets in real time. In the homeland, it is likely dynamic targeting and deliberate targeting (via air tasking orders [ATOs]) would require close coordination and integration with FAA operations.

See JP 3-30, Command and Control of Joint Air Operations, *for information on coordinating and executing ATOs, and JP 3-60,* Joint Targeting, *for information on dynamic targeting.*

e. **CO.** HD also presents unique challenges for the JFC in the selection and engagement of the cyberspace elements of targets. Since specific attribution of cyberspace threats and their geographic locations are often difficult to determine, the JFC must carefully coordinate cyberspace fires based upon best available target intelligence and the specific effects authorized in their order.

6. Movement and Maneuver in the Conduct of Homeland Defense

a. Land Operations in the Conduct of HD

(1) The GCCs with geographic HD responsibilities should anticipate, plan, and be prepared for offensive and defensive land operations. Large-scale HD operations involving maneuver forces, combined arms maneuver, and the conduct of major combat offensive or defensive operations would be an extraordinary circumstance involving extraordinary decisions by the President. However, these types of operations are planned and prepared for within the doctrinal realm of HD. HD land defense actions may include movement and maneuver, fires (for lethal and nonlethal effects), closing with and destroying an enemy, sustaining a joint force, and setting conditions for a return to peace. Specific HD land operations in support of HD may include security operations through FP tasks or CIP. Defensive land operations will make use of existing USG departments' and agencies' capabilities where possible (e.g., DHS).

(2) Land operations in the conduct of HD are planned and executed by the GCCs through their subordinate commands and either Service-specific task force HQs or JTFs. Commanders consider the scope of the OE, the specified and implied tasks, and span of control when selecting the appropriate C2 relationship. In addition, commanders should consider the interagency environment; the effect of current operations on the civilian populace; and the role of the state, tribal, and local LEAs when executing HD operations. Based upon available forces, each GCC with geographic HD responsibilities has identified subordinate commands that establish or source HQs for HD operations. The JFLCC may utilize the respective DCE assigned to the region as an advance element to provide situational awareness within the AOR and coordinate with interagency partners during DSCA and/or HD operations. Service components may utilize their respective EPLOs as an advance element to provide situational awareness within the AOR and coordinate with interagency partners during DSCA and/or HD.

(3) 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.

(4) USNORTHCOM Land Operations

(a) CDRUSNORTHCOM may employ designated land component response forces from the USA and USMC to detect, deter, prevent, and defeat threats or aggression within the AOR. USARNORTH is a Service component command that has also been designated by CDRUSNORTHCOM as the standing joint force land component command. USARNORTH could also be designated by CDRUSNORTHCOM as a JFC and provide C2 of subordinate JTFs and land forces for HD and DSCA missions. USPACOM provides a quick response force (QRF) for HD operations in the Alaska JOA. USNORTHCOM also has QRF and rapid response force (RRF) packages available for HD operations. In addition, individual states possess NG QRFs that may be used in response to an HD

situation IAW Title 32, USC, Sections 901-908, and DODD 3160.01, *Homeland Defense Activities Conducted by the National Guard*.

1. Figure III-1 shows how land forces may be provided and employed for a rapid response. When directed by the President or SecDef to conduct HD operations, CDRUSNORTHCOM can consider several initial land force options: employ a QRF or RRF, employ a JTF with OPCON over a QRF or RRF, employ a JFLCC with OPCON over a QRF or RRF, or employ USARNORTH as a single-Service HQ with OPCON of a QRF or RRF. Based on this decision, CDRUSNORTHCOM sends a request for forces (RFF) to the Joint Staff. Once SecDef approves the RFF, 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. A dedicated QRF/RRF would only be utilized in a very small or isolated incident requiring quick reaction.

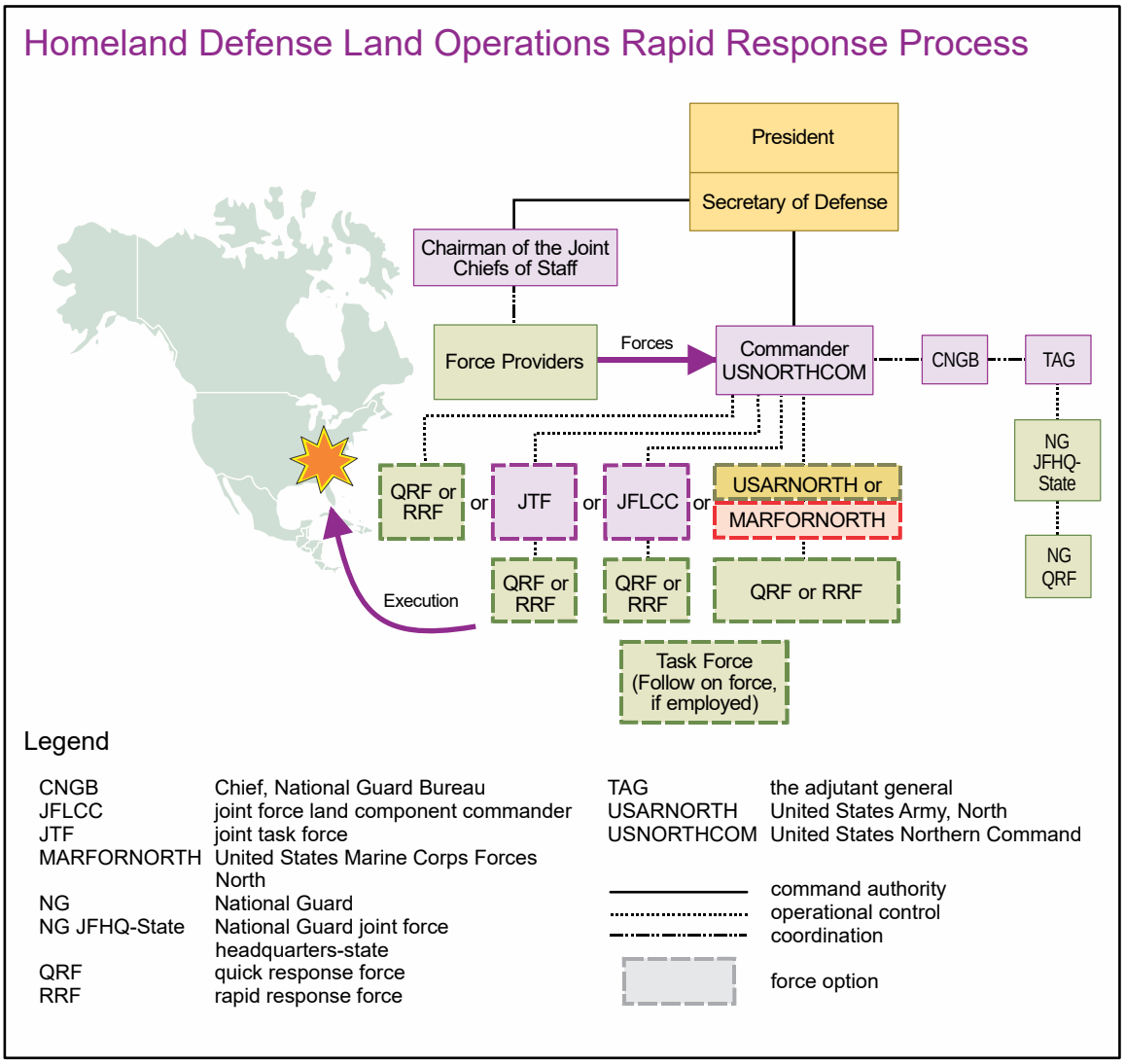


Figure III-1. Homeland Defense Land Operations Rapid Response Process

2. **USARNORTH.** CDRUSARNORTH has been designated to serve as the JFLCC for USNORTHCOM, including QRF/RRF missions. CDRUSARNORTH plans and prepares for potential HD operations through continuous coordination with other Service components; the NGB; NG JFHQ-State; JTFs; and other federal, state, local, and tribal agencies. USARNORTH-designated task forces/JTFs can provide C2 for Title 10, USC, forces designated to conduct HD missions.

3. **United States Marine Corps Forces North (MARFORNORTH).** In addition to command responsibilities, MARFORNORTH supports, coordinates, and provides advice to CDRUSNORTHCOM on the employment of Marine forces when they are attached to USNORTHCOM for the conduct of HD operations.

4. **SOCNORTH.** CDRUSNORTHCOM has OPCON of SOCNORTH, SOCNORTH provides SOF advice, support, and coordination. It is also designated the joint force special operations component commander.

(b) Although considered extraordinary, conditions may arise that require conventional land operations within the continental limits of the US (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 the requirement for interorganizational cooperation. Figure III-2 illustrates the HD land operations sustained response process. Conventional land forces are provided to CDRUSNORTHCOM per the RFF process described above and allocated to the JFLCC or the commander, joint task force (CJTF), who will have OPCON over these forces.

For more information, refer to USNORTHCOM CONPLAN 3400, Homeland Defense.

(5) **USPACOM Land Operations**

(a) CDRUSPACOM establishes JTF-HD as the HQ responsible for land HD operations on all bases and in all US territories within the USPACOM AOR. Commander, JTF-HD, receives ready forces in support of security operations, from military engagement to warfighting. These forces promote regional stability and provide crisis response.

(b) Commander, JTF-HD, has two task force structures to respond to HD/DSCA requirements. Task Force East-Hawaii is a scalable command, depending on the scope of the response as determined by USARPAC. Commander, Joint Region Marianas, is designated Commander, Task Force West-Guam, under Commander, JTF-HD.

For more information, refer to USPACOM CONPLAN 5002, Homeland Defense.

b. **Maritime Operations in the Conduct of HD.** As previously mentioned, the conduct of MHD is the responsibility of CDRUSNORTHCOM and CDRUSPACOM.

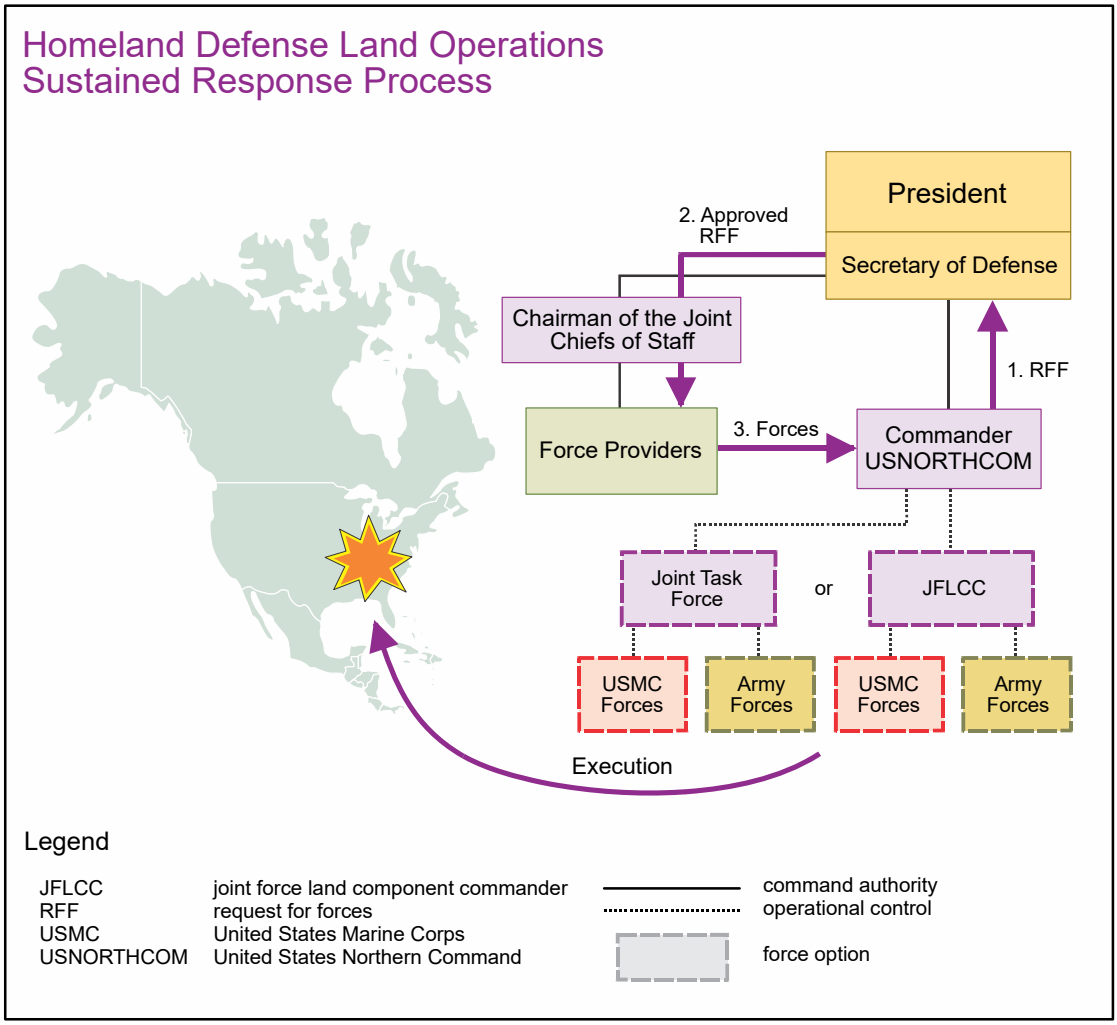


Figure III-2. Homeland Defense Land Operations Sustained Response Process

When directed by the President, responsibility for the security and defense of the homeland and its maritime approaches is shared between DOD and the USCG.

(1) Maritime operations in support of HD offer distinct challenges due to the nature of execution in or near the homeland in conjunction with interagency partners. DOD is the LFA for MHD and the USCG is the LFA for MHS. Through the relevant CCDR, DOD provides an active, layered defense; supports USCG MHS operations with DOD forces/capabilities; and defeats maritime threats to the homeland beyond the scope of MHS. Where coordination under the MOTR Plan is required, issues such as designation of lead and supporting agencies, desired national outcome, required capabilities, asset availability, and authority to act must be determined.

(2) COMUSNAVNORTH, designated as the theater JFMCC for CDRUSNORTHCOM, conducts MHD operations in the USNORTHCOM AOR and supports the USCG for MHS and the operations of the other components, as directed. JFMCC can plan and execute unilateral USNORTHCOM MHD operations while

supporting binational NORAD missions when required, including maritime warning and aerospace warning and control (air defense).

(3) COMUSPACFLT, designated as the theater JFMCC for CDRUSPACOM, conducts MHD operations in the USPACOM AOR, supports CDRUSNORTHCOM in the conduct of MHD operations in the USNORTHCOM AOR, and supports the USCG for MHS. Coordination between CCDRs for HD is addressed in specific CAAs.

(4) MHD 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 USCG MHS operations through port security and harbor defense operations; conduct mine countermeasures (MCM) operations; ensure protection of strategic sealift operations outside US ports and harbors; provide a secure environment for US and coalition forces; and support other component commanders, as directed.

For further information, see JP 3-32, Command and Control for Joint Maritime Operations. *For additional discussion of USN C2 and commander, task force, integrated air and missile defense (IAMD), see Navy Warfare Publication (NWP) 3-32,* Maritime Operations at the Operational Level of War, *and NTTP 3-32.1,* Maritime Operations Center. *For further information on the maritime composite warfare commander, see NWP 3-56,* Composite Warfare: Maritime Operations at the Tactical Level of War. *For more information, refer to USNORTHCOM CONPLAN 3400,* Homeland Defense, *and USPACOM MHD EXORD.*

(5) **MCM Operations**

(a) Enemy mining of US territorial waters can be conducted by a variety of methods (e.g., surface vessels, air, submarines, or swimmers and/or divers). Multiple agencies could be involved in a response. Guidance regarding notification, and where necessary, coordination, is provided in the MOTR protocols. Detection of mining activity is a priority for maritime surveillance systems monitoring the seaward approaches and internal waterways. DOD is responsible for all MCM operations in the maritime environment, including waters subject to US jurisdiction. Under its MHS role, the USCG is responsible for prevention and detection of mining within waters subject to US jurisdiction, which includes maritime interdiction of mine laying platforms or vessels as required. DOD also supplements the USCG's MHS role with specific DOD MCM forces, capabilities, and expertise. MCM operations can be conducted for the following reasons:

1. Bottom mapping for OE awareness prior to an event.

2. Exploratory operations to identify suspected mine threat and/or boundary of the threat area.

3. Clearance operations to locate, identify, and neutralize mine threats.

(b) Limited access areas such as safety or security zones may be required to support MCM operations. MCM forces must coordinate these regulatory functions with USCG COTPs, through the cognizant USCG area commander, when the MCM AO encompasses waters subject to US jurisdiction. DOD forces, through the senior naval officer present in command, have authority to enforce exclusionary zones established around large naval vessels, 100 feet or longer, whenever the USCG is not present in an effective MHS/LE capacity. These naval vessel protection zones are always in effect when large naval vessels transit waters subject to US jurisdiction.

For more information, see JP 3-08, Interorganizational Cooperation, *and* Title 33, Code of Federal Regulations, Parts 6 and 165.

(c) Maritime forces may support MCM operations by providing protection for MCM assets and providing logistics support for ashore staging areas in the AO. Maritime forces provide aircraft and surface vessels in order to protect MCM forces from harassment or attack. Logistics support to MCM forces is limited to messing, berthing, and potable water supplies. In the event logistics support is required, consideration should be given to basing MCM assets with or adjacent to maritime forces to economize security and logistics support.

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

(6) **Sea Lines of Communications and 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. During a declared MHD mission, USCG MHS operations will support military strategic sealift operations in strategic US ports, harbors, and their approaches under the national port readiness network, specifically through military outload protection operations. If the corresponding MHD mission requires USCG units conducting military outload protection under MHS authority to counter a specific MHD threat, the applicable USCG area commander and JFMCC may request the transfer of forces to CGDEFOR as needed to defeat the threat under SROE.

For more information on USCG military outload protection, see COMDTINST M16600.6, Maritime Security and Response Operations (MSRO) Manual.

(7) **Maritime Interception Operations (MIO), Expanded Maritime Interception Operations (EMIO), and Boarding**

(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 boarding is noncompliant or opposed, subject to applicable ROE. The specific political, geographic, and tactical factors and the legal authority on which the MIO are based influence the enforcement procedures. Under certain circumstances, MIO conducted by a JFC may lead to a DOD-initiated MOTR process if additional interagency authorities, capabilities, disposition, and/or application of US jurisdiction are in the USG's interest.

(b) MIO are a USN core mission. Most USN ships and USCG cutters are capable of conducting compliant and certain types of noncompliant boardings. USN ships and USCG cutters must be augmented by other forces (e.g., SOF, USMC maritime raid forces, USCG LE detachment or maritime security response team) to conduct certain types of noncompliant boardings or to conduct opposed boardings.

For more information on compliant, non-compliant, and opposed boardings, see NTTP 3-07.11M/CGTTP 3-93.3/Marine Corps Interim Publication (MCIP) 3-33.04, Visit, Board, Search, and Seizure Operations.

(c) Maritime forces may also be tasked to conduct EMIO. EMIO are authorized by the President through SecDef to deter, degrade, disrupt, or prevent attacks against the US and its allies. EMIO involve interception of targeted personnel or materiel that poses an imminent threat to the US and its allies. EMIO may be implemented without sanctions and may involve multinational forces. For further reference, see NTTP 3-07.11M/CGTTP 3-07.11/MCIP 3-33.04, *Visit, Board, Search, and Seizure Operations.* See also JP 3-03, *Joint Interdiction.*

(8) **Littoral Operations.** Both MHS and MHD operations may occur simultaneously in the homeland's littoral areas. The USCG conducts MHS operations at all times to prevent, disrupt, and respond to terrorism, sabotage, espionage, or subversive acts. During a declared MHD mission, MHD in the littoral regions includes maritime forces conducting harbor approach defense to protect shipping in designated harbor approach areas, to assure unimpeded use of harbor approach areas and application of lethal and nonlethal force under SROE to deny the use of these areas by enemy forces.

c. **Air Operations in HD Operations.** NORAD is assigned the mission of aerospace control (including air sovereignty and air defense) of the airspace of the US and Canada. NORAD routinely maintains forces on alert for homeland air defense, CM defense, and aerospace control alert missions against long-range incursions. Air and missile defenses are discussed under paragraph 6, "Protection." USNORTHCOM is generally responsible for all other air operations supporting land and MHD outside the scope of the NORAD Agreement.

(1) NORAD/United States Element, North American Aerospace Defense Command (USELEMNORAD) should also be prepared to intercept and defend against terrorist air threats, even when the intent to harm the US is uncertain. These threats could include commercial or chartered aircraft, general aviation, ultra-light aerial vehicles,

unmanned aerial systems (from commercial to radio-controlled aircraft), or even balloons. Early detection and successful interception of these types of potential threats requires cooperation and very close coordination with interagency partners, including FAA and DHS.

(2) Aerospace defense operations within the homeland provide some unique concerns for CDRUSNORTHCOM and CDRUSPACOM.

(a) **Size.** The GCCs' HD responsibilities include vast areas of airspace, land masses, and water. In particular, North America is a huge land mass with multiple avenues of approach that an adversary could use to advantage.

(b) **Control of Airspace.** US airspace is under the control of the FAA. Civilian control of airspace, as well as other security functions vital to the homeland, requires coordination among several USG departments and agencies.

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

(d) **Duration.** Defense of the homeland, involving US and Canadian air, land, and maritime forces, is on a continuous operational basis in peacetime as well as in times of crisis.

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

(3) SecDef has designated CDRNORAD as the supported commander for aerospace warning and aerospace control aspects of HD within the NORAD OA.

(a) 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.

(b) The OA includes the portions of the homeland that fall within the USNORTHCOM AOR, 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.

(4) The missions of NORAD and USNORTHCOM are complementary. NORAD conducts aerospace defense missions and operations within the USNORTHCOM AOR and provides warning of all airborne threats, to include aircraft and missile attack, as well as maritime threats. USNORTHCOM conducts US-only air, land, and maritime defense. The commands work side-by-side and coordinate on many issues. NORAD 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 air and space defense of Canada and HD of the US by providing aerospace warning and airspace control and maritime warning for North America.

(a) ONE. ONE is the operation covering aerospace warning and control aspects of HD for CONUS, Alaska, the US Virgin Islands, and Puerto Rico. As the binational element of this operation, NORAD is tasked to support ONE by employing the forces and C2 necessary to protect these areas from air attack. USPACOM provides C2 (through Pacific Air Forces) for ONE support to Hawaii and US territories in USPACOM's AOR.

(b) The authority and decision to engage is made at the highest levels of command. NORAD constantly refines its procedures and coordinates with DHS; Public Safety Canada; Emergency Preparedness Canada; the FAA and its Canadian equivalent, NAV CANADA (air traffic control agency); and with civilian LE organizations and other government agencies within the US and Canada.

For a more complete description of the NORAD missions, organization, and structure, see Appendix C, "North American Aerospace Defense Command, Missions, Organization, and Structure." For more information, refer to NORAD CONPLAN 3310, Aerospace Defense & Maritime Warning, *and ONE EXORD.*

d. **Space Operations in the Conduct of HD.** The region in space above the US and other countries cannot be owned or possessed like territory. However, it is USG policy 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. DOD defense critical infrastructure (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 the US's 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.

(1) **Enabling Capabilities.** Military space operations bring enabling capabilities and information to the JFC such as initial threat detections and locations, global communication, positioning, navigation, timing, real-time weather, high-resolution imagery, and signals intelligence (SIGINT). 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; international; and other federal, state, tribal, and local partners in support of HD operations. This information from space systems provides decision makers advance warning to prevent, prepare for, respond to, and recover from threats to the homeland.

(2) **Roles and Responsibilities**

(a) CDRUSSTRATCOM develops desired characteristics and capabilities and advocates, plans, and conducts space operations. These responsibilities are to:

1. Provide warning and assessment of space attack.

2. Support NORAD by providing the missile warning and space surveillance necessary to fulfill the US commitment to the NORAD Agreement.

3. Serve as the single point of contact for military space operational matters, except as otherwise directed.

4. Provide 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 CCDRs.

5. Coordinate and conduct space planning.

(b) CDRUSSTRATCOM established the JFCC Space to serve as the single point of contact for operational space matters, including planning, tasking, directing, and executing space operations using assigned space forces.

(c) GCCs with geographic HD responsibilities are the supported commanders responsible for conducting HD operations within their respective AORs. These include:

1. Communicate space capability requirements to JFCC Space through the command's SCA when acting in an HD capacity.

2. Provide FP for space assets located within their respective AORs.

(3) **Integration of Civilian Space Capabilities.** HD is a high-priority activity which requires 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 provides an integral part of the total US space capabilities. The private sector and other civilian space capabilities are essential to the effectiveness of the US's ability to successfully accomplish the HD mission.

For additional information, refer to JP 3-14, Space Operations.

e. **CO in the Conduct of HD.** The US conducts operations, including HD, in a complex, interconnected, and increasingly global OE. Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

(1) **The NMS for CO and the DOD Cyber Strategy** offers a comprehensive strategy for DOD to enhance US superiority in cyberspace. The NMS for CO addresses three main roles: defense of the nation, national incident response, and CIP. GCCs with geographic HD responsibilities should ensure unified action at the theater level for CO.

This includes coordinating with multinational and interagency partners as outlined in strategy, policy, and agreements. DOD Cyber Strategy instructs DOD to be prepared to defend the US homeland and US vital interests from disruptive or destructive cyberspace attacks of significance consequence. JFCs employ cyberspace capabilities to achieve objectives in or through cyberspace. Such operations include OCO, DCO, and protection of the DODIN.

(2) **National Infrastructure Protection through CO.**

(a) The security and effective operations of US critical infrastructure—including energy, banking and finance, transportation, communication, and the defense industrial base (DIB)—rely on cyberspace (e.g., industrial control systems and information technology are vulnerable to disruption or exploitation).

(b) DHS's National Cybersecurity and Communications Integration Center is a continuous cyberspace situational awareness, incident response, and management center that is a national nexus of cyberspace and communications integration for the USG, IC, and LEAs.

For more information on DHS's role in CO, see https://www.dhs.gov/topic/cybersecurity.

(c) As LFA for the maritime transportation system under the DHS National Infrastructure Protection Plan, the USCG leads overall unity of effort required to protect the maritime transportation sector from cyberspace attacks while supporting DODIN operations.

For more information on USCG roles in CO, see the USCG Cyber Strategy, *at https://www.uscg.mil/seniorleadership/DOCS/cyber.pdf.*

(3) NG support to CO at the state level consists of CO squadrons within the ANG and cyber protection teams within the ARNG.

For additional information, refer to JP 3-12, Cyberspace Operations.

f. **Information Operations (IO) in the Conduct of HD.** IO are the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of threats while protecting our own. Information-related capabilities include some already discussed separately, such as space operations and CO, but also includes such capabilities as MISO, electronic warfare, combat camera, operations security, and military deception. IO complements HD movement and maneuver in all domains by generating effects in the information environment that give the JFC a decisive advantage in any and all of its dimensions: physical, informational, and cognitive. IO also plays a significant role in the JFC's communication synchronization.

(1) The information environment supports the HD framework. The information environment is made up of the physical, informational, and cognitive dimensions. The physical dimension is composed of C2 systems, key decision makers, and supporting

infrastructure that enable individuals and organizations to create effects. The informational dimension specifies where and how information is collected, processed, stored, disseminated, and protected. The cognitive dimension encompasses the minds of those who transmit, receive, and respond to or act on information. Information-related capabilities such as MISO as part of commander's communication synchronization are used to create effects in the information environment.

(2) **DODIN.** As part of the overall information environment, the DODIN represents the 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 whether interconnected or stand alone. The DODIN includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services and national security systems.

(a) Consistent with laws and policy, Services, DOD agencies, and non-DOD agencies should provide capabilities to support CCMD requirements to ensure the interoperability, availability, and shared situational awareness and understanding of the HD information environment. This includes capabilities to detect, deter, prevent, and defeat virtual and physical attacks against DODIN infrastructure that directly or indirectly supports HD missions.

(b) There are three primary aspects to providing available and effective systems to execute HD. These are: providing a reliable, robust HD communication system; improving information sharing among HD mission partners; and assuring and defending the critical DODIN infrastructure against threats and aggression.

For more information on DODIN, see JP 3-12, Cyberspace Operations, *and JP 6-0,* Joint 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 their 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 common operational picture (COP) facilitates decentralized execution in rapidly changing OEs and should be shared among appropriate agencies, to include LE, to ensure consistent situational awareness.

2. 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.

3. The GCC AORs 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. DOD communications systems will serve as the backbone in support of HD operations. Systems that are scalable, interoperable, and complementary with those used by multinational and civilian partners, will be essential to augment traditional intelligence collection 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, local, and tribal responders; international organizations and NGOs; and private sector responders to operate on the same bandwidth to facilitate interoperability. Planning for the secure integration of internationally donated telecommunications resources, including hardware and SATCOM bandwidth, must be conducted in the event the USG accepts offers of international aid.

4. The Radio Amateur Civil Emergency Service provides emergency communications for civil defense organizations as authorized by Title, 47, Code of Federal Regulations, Part 97, Section 97.407.

For more information on spectrum management, see JP 6-01, Joint Electromagnetic Spectrum Management Operations, *and for more information on joint electromagnetic spectrum operations, see JDN 3-16,* Joint Electromagnetic Spectrum.

g. **Joint Reception, Staging, Onward Movement, and Integration (JRSOI).** JRSOI is the essential process that assembles personnel, equipment, and materiel after movement or deployment into forces capable of meeting the CCDR's operational requirements. In the USNORTHCOM AOR, portions of JRSOI are not regarded as discrete steps necessary for HD operations.

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

(2) Reception operations include all those functions required to receive and clear unit personnel, equipment, and materiel through the BSI or reception area. For HD operations within the USNORTHCOM AOR, the personnel, equipment, and materiel will likely originate from within the JOA. In that case, personnel, equipment, and materiel are already accounted for at the home base, making the home base essentially the point of departure. Component support plans should address processes for in-place personnel reporting to the CJTF.

(3) Similar to reception, personnel, equipment, and materiel to be employed for HD operations within the USNORTHCOM AOR may stage within the confines of their home installation. Otherwise, arriving personnel, equipment, and materiel may be temporarily held at a BSI or other location while they are staged, assembled, and organized into forces and capabilities in preparation for onward movement.

(4) Onward movement is the process of moving units and accompanying materiel from reception facilities, marshalling areas, and staging areas to tactical assembly areas (TAAs), OAs, or other theater destinations. Because units and forces 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 reception and staging activities at the home base. When a unit or force is not geographically close to an OA and a TAA other than the home base is desired, then discrete, onward movement activities would be required. Oftentimes, a TAA would be located at a designated BSI that would provide logistics support and be located near the OA.

(5) Integration is the synchronized handoff of units into an operational commander's force prior to mission execution. HD operations within the USNORTHCOM AOR often require complex C2 structures. Special attention to integration, synchronization, and coordination is required. Refer to Appendix A, "Relationships Between Homeland Security, Homeland Defense, and Defense Support of Civil Authorities."

h. **Movement in Support of HD.** Deployment operations within the homeland can be extremely time compressed. The national importance of these missions is reflected in the elevated movement priorities that can be invoked by the President or SecDef. United States Transportation Command (USTRANSCOM) can quickly assemble aircraft and flight crews for operations where expedited passenger movement is required. Surface transportation (commercial and organic) can be a viable option in those situations where the distance between the home station and the OA is relatively short. Coordination with NGB is essential when using ANG/ARNG assets for support of HD. In some instances, state and federal forces may be in the same OA. Coordination between state and federal forces should occur to achieve unity of effort.

For more information on JRSOI, see JP 3-35, Deployment and Redeployment Operations.

7. Protection

The protection function focuses on conserving the joint force's fighting potential in four primary ways: **active defensive** measures employed outside the defended area that protect the joint force, its information, its bases, necessary infrastructure, and lines of communications from an enemy's attack by employing limited offensive action and counterattacks; **passive defensive** measures employed within a defended area that make friendly forces, systems, and facilities difficult to locate, strike, and destroy and to minimize damage from enemy attacks; **application of technology and procedures** to reduce the risk of friendly fire; and **emergency management and response** to reduce the loss of personnel and capabilities due to an all-hazards incident. It includes, but extends beyond, FP to encompass protection of US noncombatants; the forces, systems, and civil infrastructure of friendly nations; and other USG departments and agencies, international organizations, and NGOs. Planning for HD includes combating terrorism, criminal enterprises, environmental threats/hazards, and CO. **Joint intelligence preparation of the OE must be conducted to ensure adequate planning and implementation of protection**

measures. A separate directorate may be established for interagency coordination for HD planning due to intelligence limitations in the homeland and the vast amount of information the interagency partners can provide.

For additional information on the protection function, see JP 3-0, Joint Operations. *For more information on DOD AT and FP programs, refer to DODI 2000.12,* DOD Antiterrorism (AT) Program; *DODI O-2000.16, Volume 1,* DOD Antiterrorism (AT) Program Implementation: DOD AT Standards; *DODI O-2000.16, Volume 2,* DOD Antiterrorism (AT) Program Implementation: DOD Force Protection (FPCON) System; *and JP 3-07.2,* Antiterrorism.

a. **IAMD.** IAMD is the integration of capabilities and overlapping operations to defend the homeland and US national interests, protect the joint force, and enable freedom of action by negating the adversary's ability to create adverse effects from their air and missile capabilities. Due to policy differences and legal agreements and physical characteristics of threats, air and missile defense are not integrated in the same manner as air and missile defense in other GCCs' AORs. NORAD, USNORTHCOM, and USPACOM, share the missions of air defense and missile defense for the homeland, and C2 of forces are integrated at the CCDR level. The NORAD and USNORTHCOM Command Center coordinates air and missile fires. As explained in Chapter I, "Fundamentals of Homeland Defense," CDRNORAD is tasked to provide aerospace warning, aerospace control, and maritime warning for North America, while CDRUSNORTHCOM is tasked to provide BMD and all other forms of HD within the AOR. Although CDRUSNORTHCOM is normally designated CDRNORAD, the commands are distinct entities. CDRUSPACOM is responsible for HD within the USPACOM AOR, including air and missile defense. USPACOM supports USNORTHCOM for certain limited BMD defense options, for example the defense of Hawaii.

For further discussions on missile defense, refer to JP 3-01, Countering Air and Missile Threats.

(1) **Air Defense.** CDRNORAD is tasked to provide aerospace control for North America, which includes surveillance and control of Canadian and US airspace, as well as ensuring air sovereignty and air defense against aircraft and CMs. NORAD has the responsibility to protect the US and Canadian homelands against military or civilian airborne threats.

For more detailed discussions on air and missile defense, refer to JP 3-01, Countering Air and Missile Threats.

(a) Aircraft. To accomplish the aerospace control mission, NORAD uses a network of satellites, ground-based radar, airborne radar, and fighters to detect, intercept and, if necessary, engage any air-breathing threat to Canada and the US.

(b) CMs. CMs are air-breathing threats capable of delivering a full range of warheads, from conventional to WMD. Because they are air breathing threats, CMs are

part of the air defense role executed by NORAD. CMs present significant detection difficulties due to standoff range and very small radar cross-section.

(c) Other Threats. UA are a growing threat to the US and Canadian homelands. Larger UA threats are prosecuted in the same manner as other military or civilian-based air threats. Smaller UA threats are addressed through cooperation efforts with federal, state, and local agencies. A terrorist attack using an aircraft as a weapon continues to be a threat to the homeland.

(2) **NCR-IADS.** Defense of the NCR is a special case of air defense in the homeland. DOD employs an integrated air defense system (sensors, weapons, visual warning system, C2 systems, and personnel) as part of the around-the-clock, multilayered, military, and interagency effort to protect the NCR.

(a) The NCR-IADS augments ONE fighter defenses by providing in-place assets which are in a quick reaction posture to protect the seat of the USG, as well as other key locations in the NCR from air attacks.

(b) The Transportation Security Administration (TSA) and other elements of DHS, as well as DOJ and DOT, conduct significant aviation security efforts throughout the US 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 regarding the actions of their defense partners. The NCRCC is a coordination center, and no command or control of forces occurs. NCRCC 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 LEAs and the Joint Air Defense Operations Center (JADOC) also participate at the NCRCC when threats or circumstances warrant.

For additional information on air operations, refer to JP 3-01, Countering Air and Missile Threats; *JP 3-30,* Command and Control of Joint Air Operations; *and JP 3-52,* Joint Airspace Control.

(3) **BMD.** BMD capabilities are designed to detect, deter, prevent, and defeat adversary ballistic missile threats and help protect the US domestic population and critical infrastructure. US homeland BMD includes not only the means for active and passive defenses, but the capability to strike in retaliation or to preempt the launch of a missile threat. For HD, there are BMD capabilities against limited attacks by rogue states using ICBMs and capabilities against threats from short-range ballistic missiles, medium-range ballistic missiles, and intermediate-range ballistic missiles. ICBM threats are deterred by US capabilities that include global strike. BMD is a key element of HD. However, BMD activities do not include defense against CMs or tactical air-to-surface missiles.

(a) **BMD System.** The BMD system includes the sensors (air, land, sea, and space), anti-ballistic missiles, communications, and C2 for launch warnings and assessment for all categories of ballistic missile launches, whether targeted against the homeland or other AORs. The ground-based midcourse defense (GMD) element of the BMD system provides USNORTHCOM the capability to engage and destroy limited intermediate- and long-range ballistic missile threats in space to protect the US. The GMD system is composed of ground-based interceptors and associated sensors and fire control systems. The ground-based interceptor is a multi-stage, solid fuel booster with a lethal payload. Fire control systems consist of redundant fire control nodes, interceptor launch facilities, and a communications network.

(b) **BMD Roles and Responsibilities.** GCCs are responsible for planning and executing BMD against ballistic missile threats that target their AORs, to include threats that cross AOR boundaries. This is supported by shared situational awareness, integrated battle management, adaptive planning, and accurate and responsive battle damage assessment. The following have specific BMD responsibilities to support HD.

1. USNORTHCOM and USPACOM have specified HD responsibilities and authority to deter ballistic missile attacks on the US, its territories, and bases within their respective AORs, and other areas as directed by the President or SecDef. In coordination with other CCMDs, they synchronize operations to detect, deter, prevent, and defeat ballistic missile attack on the homeland. Should deterrence fail, and/or as directed by the President or SecDef, they employ BMD forces to protect the US against ballistic missile attacks. CDRUSNORTHCOM, in coordination with CDRUSPACOM, has responsibilities within the USPACOM AOR to ensure homeland BMD. Employing the GMD system requires centralized planning and direction by CDRUSNORTHCOM and centralized execution due to the required positive direction from the weapons release authority (WRA). WRA is the authority delegated from the President to use ground-based interceptors against ICBM threats. CDRUSPACOM is the supported commander for homeland BMD that does not include GMD.

2. The NG provides BMD-trained personnel to USNORTHCOM. The 100th Missile Defense Brigade (Ground-based Midcourse Defense) is a multi-component brigade consisting of Active Component (AC) Army and ANG Soldiers in Colorado, California, and Alaska who are tasked with the mission of defending the homeland from limited ICBM attacks. The 100th operates the GMD while under OPCON of CDRUSNORTHCOM.

(4) **Space Operations and BMD.** 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, refer to JP 3-14, Space Operations.

b. **CIP**

(1) **DCI.** DCI consists of 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 include infrastructure such as installations, facilities, ports, bridges, power stations, telecommunication lines, and pipelines, most of which will not be located on USG property.

(a) Examples of DCI include strategic military bases, ports of embarkation/ports of debarkation, and mobilization staging and storage areas, plus rail and trucking transportation centers. 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 as a constitutional exception to the PCA. 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. State and local governments also are interested in securing CI/KR, so coordination of physical/virtual protection measures should be part of the USG efforts.

(b) **Mission Assurance and the DIB.** Mission assurance is the process to protect or ensure the continued function and resilience of capabilities and assets—including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains—critical to the execution of DOD mission-essential functions in any OE or condition. Mission assurance focuses on the "protection," "continued function," and "rapid reconstitution" of critical assets which support mission essential functions, rather than the execution of these missions themselves. Threats to non-DOD government and commercially owned infrastructure, facilities, and capabilities, to include the DIB, can jeopardize DOD HD mission execution. Mission assurance focused only on assessing and protecting, or enhancing resilience against DOD-specific vulnerabilities, will fail. Thus, it is necessary to comprehensively assess and mitigate risk in a way that accounts for DOD dependence on civilian assets and systems and the cascading consequences of their disruption. These include, but are not limited to, transportation networks, global supply chains, electric power, telecommunications, and information technology infrastructures. Simultaneously, one must also recognize the lead role of other USG departments and agencies, especially DHS, the Department of Energy (DOE), and DOT, in coordinating risk mitigation for threats to civilian infrastructure.

(c) All CCDRs, in coordination with DOD asset owners, DOD components, and the defense infrastructure sector lead agents, take action to prevent or mitigate the loss or degradation of DOD-owned DCI within their assigned AOR.

For more information concerning CIP and the DCIP, see DODD 3020.40, Mission Assurance (MA), *and DODI 5220.22,* National Industrial Security Program.

(2) **CI/KR.** As stated in the Critical Infrastructure and Key Resources Support Annex to the NRF, "CI/KR includes those assets, systems, networks, and functions—physical or virtual—so vital to the US that their incapacitation or destruction would have a debilitating impact on HS, national economic security, public health or safety, or any

combination of those matters. Key resources are publicly or privately controlled resources essential to minimal operation of the economy and the government." An attack on CI/KR could significantly disrupt the functioning of government and business alike and produce cascading effects far beyond the physical location of the incident. Although DOD's role is normally one of administrative and logistical support to DHS or another sector-specific agency through DSCA or direct MHS support, in certain circumstances, the President may direct DOD to provide military protection to CI/KR.

For further information, see PPD-25, Guideline for US Government Interagency Response to Terrorist Threats or Incidents in the US and Overseas; *HSPD-7,* Critical Infrastructure Identification, Prioritization, and Protection; the National Strategy for Physical Protection of Critical Infrastructure and Key Assets; the National Infrastructure Protection Plan; *and HSPD-23/NSPD-54,* US Cyber Security Policy. *See also the NRF at https://www.fema.gov/national-planning-frameworks.*

c. **CWMD**

(1) WMD capabilities are of particular concern to the USG. Threats may use WMD as a tool to inflict mass casualties on homeland civilian populations or cause disruption or destruction to critical infrastructure.

(2) CWMD, as a part of HD, is a global mission with potential consequences that cross AOR boundaries. CWMD requires an integrated and synchronized effort from numerous interagency and multinational partners for effective mission accomplishment. CWMD is a continuous effort that requires a coordinated, unified effort to curtail the conceptualization, development, possession, proliferation, use, and effects of WMD-related expertise, materials, and technologies.

(3) CWMD contributes to HD through an integrated approach to reduce incentives to pursue, possess, and employ WMD; increase the barriers to WMD development, acquisition, advancement, proliferation, and use; manage WMD risks emanating from hostile, fragile, or failed states, non-state actors and safe havens; and deny the effects of current and emerging WMD threats through layered, integrated defenses.

(4) CWMD includes DOD CBRN Response Enterprise, which has the primary mission to detect and respond to WMD incidents in the homeland.

For more information on CWMD, see JP 3-40, Countering Weapons of Mass Destruction; *JP 3-41,* Chemical, Biological, Radiological, and Nuclear Response; *and JP 3-11,* Operations in Chemical, Biological, Radiological, and Nuclear Environments.

d. **CO and DODIN Operations.** Each CCMD, Service, and DOD agency contributes to overall HD cybersecurity by rigorous implementation of cybersecurity policies and procedures. CCMDs, Services, and DOD agencies employ appropriate cyberspace security actions to prevent intrusions and defeat other adversary activities on DOD networks and systems that are not a part of what is specifically defined as the DODIN. There are subordinate HQs of USCYBERCOM that execute C2 of the Cyber Mission Force and other cyberspace forces. These include the Cyber National Mission Force-Headquarters, the

Joint Force Headquarters-Department of Defense Information Network, joint force HQ-cyberspace, and Service cyberspace component commands. Each of the Service cyberspace component commanders is dual-hatted by Commander, USCYBERCOM, as a commander of one of the four joint force HQs-cyberspace to enable synchronization of CO C2. In addition, there are other centers and staff elements that further enable unity of command for CO. Due to the close interdependencies DOD and IC components have on each other's networks, it is essential reporting procedures be in place to ensure rapid coordination in cyberspace defense. Reporting on IC networks comes from the IC through USCYBERCOM and is shared with the CCDRs with geographic HD responsibilities.

For more information on CO, see JP 3-12, Cyberspace Operations.

e. **FP.** GCCs are responsible for FP within their respective AORs. 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, including those with AORs which contain geographic areas of the homeland. Force health protection (FHP), the protection component of health services, complements FP and includes all measures to ensure a healthy and fit force, prevent injury and illness, and protect the force from health hazards.

(1) **AT and FP.** GCCs have overall AT responsibility within their respective AORs, except for those DOD elements and personnel for whom another commander has security responsibility pursuant to law or a memorandum of agreement. The AT program is designed to prevent and detect terrorist attacks against DOD personnel, their families, facilities, resources, installations, and DCI, as well as to prepare to defend against, and plan the response to the consequences of, terrorist incidents. TACON (for FP) applies to all DOD personnel assigned, permanently or temporarily; transiting through; or performing exercises or training in the GCC's AOR. GCCs have the authority to modify FP conditions for covered individuals. CDRUSNORTHCOM has overall DOD AT program and FP responsibility in CONUS. USNORTHCOM's FP mission and AT program are outlined in the USNORTHCOM Instruction 10-222, *Force Protection Mission and Antiterrorism Program*.

For additional information, see JP 3-07.2, Antiterrorism.

(2) **FHP.** FHP provides the framework for optimizing health readiness and protecting Service members from all health threats. In general, US states and territories are normally at low risk for endemic diseases, although pandemic disease outbreaks have the potential to rapidly place the US military and wider population at risk. Additionally, some areas within the homeland are heavily industrialized and have the potential for deliberate or accidental release of a large variety of toxic industrial chemicals/materials at production sites and during transportation. Furthermore, WMD attacks pose unique FHP risks due to the health effects and threats of CBRN agents. Thus, man-made hazards (deliberate or accidental) may present the greatest potential health risk to forces conducting HD operations.

For more on FHP, see JP 4-02, Joint Health Services.

f. **Combating terrorism** includes AT and CT actions taken to oppose terrorism throughout the entire threat spectrum. The broad USG strategy is to continue to lead an international effort to deny violent extremist organizations the resources and functions they need to operate and survive. CT activities and operations are taken to neutralize terrorists, their organizations, and networks in order to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals. DOD's strategy for combating terrorism implements the following objectives from the *National Strategy for Combating Terrorism,* which are derived from the NSS:

(1) Thwart or defeat terrorist attacks against the US, its PNs, and its interests.

(2) Attack and disrupt terrorist networks abroad so as to cause adversaries to be incapable or unwilling to attack the US homeland, allies, or interests.

(3) Deny terrorist networks access to WMD.

(4) Establish conditions that allow PNs to govern their territory effectively and defeat terrorists.

(5) Deny a hospitable environment to violent extremists.

For more information on countering threat networks and CT, refer to JP 3-25, Countering Threat Networks, *and JP 3-26,* Counterterrorism.

8. Sustainment

a. **Personnel**

(1) The core functional responsibilities of the manpower and personnel directorate of a joint staff (J-1) are accomplished during any HD or other operation and are tailored to meet mission-specific requirements.

(2) **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 exceptions may apply to 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. For example, units deploy from their home stations instead of from a unique designated port of embarkation. Service personnel elements supporting home station deployments must ensure all processing and reporting requirements are met prior to unit deployment. In specific circumstances, such as operations in a CBRN environment, the employing CJTF may establish a joint personnel reception center to ensure arriving units are ready for employment.

(b) **Individual Augmentation.** Tactical capabilities are provided by organic unit force structure wherever possible, and the request vehicle for this type of requirement is the RFF. Individual subject matter experts may be required to augment operational C2 organizations. The request vehicle for joint individual augmentation is a CCDR-approved and Joint Staff-validated joint manning document. Joint individual augmentees are not QRFs but are a result of planning for contingencies, if the contingency for the unique task organization is projected to last longer than 90-120 days. For detailed guidance, refer to CJCSI 1301.01, *Joint Individual Augmentation Procedures.*

(c) **Personnel Accountability in Conjunction with Disasters.** Attacks on the US can affect DOD personnel and their dependents. Service components account for and report the status of all DOD-affiliated military and civilian personnel, including contractors 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 Manmade Disasters. *For detailed guidance on personnel support, see JP 1-0,* Joint Personnel Support.

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 US. More specifically, the exceptions apply to the USNORTHCOM AOR.

(1) JP 1, *Doctrine for the Armed Forces of the United States,* states "exercise of directive authority for logistics by a CCDR includes the authority to delegate authority to issue directives to subordinate commanders" and "CCDRs exercise COCOM over assigned forces." Within the USNORTHCOM AOR, the CDRUSNORTHCOM executes OPCON or TACON over attached forces, normally without directive authority for logistics. Given the robust capabilities within each Service component, DOD combat support agency (CSA), and the commercial contracting infrastructure in USNORTHCOM AOR, directive authority for logistics is not necessary to execute the HD mission. CDRUSNORTHCOM has theater- and operational-assigned and allocated logistical forces and capabilities executing OPCON of those forces via Service component HQs. CDRUSNORTHCOM may still exercise directive authority for logistics in responding to an HD threat; the President or SecDef may also extend this authority to attached forces when transferring those forces for a specific mission.

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

(3) In the case where multiple agencies, PNs, international organizations, NGOs, and private sector entities are involved in HD operations, each is ultimately responsible for

BASE SUPPORT INSTALLATION

A base support installation (BSI), when approved by the Secretary of Defense, serves as the main logistical hub for military support operations in the US and its territories. Although joint forces may arrive through multiple reception sites near the joint operations area (JOA), generally the logistics support is provided by the BSI. Typically, most forces will deploy through, and the majority of sustainment will be positioned at, the BSI. A BSI will normally have the following characteristics: a logistics requisitioning activity; an airfield (or nearby airport) 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 (e.g., billeting, food service, and force protection); and proximity to the JOA to remain responsive and flexible to the needs of the joint force.

Various Sources

providing logistics support for their own personnel. However, the GCC should strive to integrate efforts through the use of acquisition and cross-servicing agreements along with associated implementing arrangements to ensure needed logistics support. Optimizing the capabilities should result in greater flexibility, more options, and more effective logistics support. In allocation of logistics support to HD activities, unit force activity designators should be reviewed for possible improvement or downgrade based on mission criticality.

(4) **Logistic Capabilities.** Responsibilities for logistics as described in JP 4-0, *Joint Logistics,* apply to HD operations as follows:

(a) **Supply.** USNORTHCOM will synchronize Service component and CSA logistics supply capabilities to support the joint force.

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

(c) **Deployment and Distribution.** HD airlift priorities are outlined in CJCSI 4120.02, *List of Priorities -- DOD Transportation Movement Priority System.* The national importance of included mission areas is reflected in the elevated movement priorities that can be applied to them by the President or SecDef. For operations that demand expedited movement, CDRUSTRANSCOM maintains on-call readiness levels necessary to meet CDRUSNORTHCOM mission requirements. The North American Aerospace Defense Command and United States Northern Command Deployment and Distribution Operations Cell (NDDOC) is embedded within the Joint Logistics Operations Center and is composed of personnel from NORAD, USNORTHCOM, and national partners as required (e.g., USTRANSCOM, Defense Logistics Agency [DLA], the Services, and other organizations). It is established as directed by CDRUSNORTHCOM to support HD (and DSCA) operations and operates under the direction of the NORAD and USNORTHCOM logistics and engineering directorate. 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) **Combat Service Support (CSS).** CSS is a Service responsibility. It enhances combat capability and improves productivity by providing life-sustaining and essential service. CSS also provides critical supply, maintenance, and transportation services to enable the operating force to conduct HD missions. Additionally, CSS supports force reception and beddown during military operations. The primary focus of the CSS effort in HD is to sustain and assist employed DOD forces. The primary method for common-user logistics support or sustainment is normally accomplished through the supporting BSI.

(e) **Operational Contract Support (OCS).** OCS provides the CCDR the tools and processes to manage the variety of services that may be required. Within OCS are contract support integration, contractor management, and contracting support.

For more information on OCS, see JP 4-10, Operational Contract Support, *and DODI 3120.41,* Operational Contract Support.

c. **Engineering.** Military engineering support may be required simultaneously for HD and DSCA operations. The primary focus of the engineering effort will be to sustain and assist DOD forces employed in HD. The secondary effort will be DSCA, when requested and approved IAW DOD guidance and applicable plans. The scope of engineering support for HD focuses on mobility, FP construction, force beddown, geospatial engineering, and emergency stabilization and repair of damaged DOD critical infrastructure. The duration and scope of DOD engineer involvement will be directly related to the severity and magnitude of the threat, situation, or event. Engineer planners should develop plans with forces capable of initial tasks and priority of effort. Engineer efforts in HD may evolve into DSCA engineer actions. Whether the focus is HD or DSCA, engineering missions may require the use of Service members or contracted services.

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

d. **Environmental Considerations.** Military commanders employ environmentally responsible practices that minimize adverse impacts to human health and the environment. During all operations, plans will be developed to reduce or eliminate negative impacts on the environment and to minimize negative impacts to mission accomplishment caused by environmental degradation. 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; however, compliance with applicable federal, state, tribal, and local laws to the maximum extent possible during crisis

circumstances is still a DOD objective. Commands will initiate actions to curtail further environmental damage and to resolve environmental impacts.

For additional information on environmental considerations, see JP 3-34, Joint Engineer Operations.

e. **Mortuary Affairs (MA).** USNORTHCOM and USPACOM may be required to conduct MA for US, allied, or adversary casualties of HD operations.

See JP 4-06, Mortuary Affairs, *for details on employment of DOD MA assets in DSCA, mass-fatality management, CBRN response, and HD operations.*

f. **Religious Support (RS).** RS during HD missions is conducted by a religious support team (RST) consisting of one chaplain and an enlisted assistant of the same service. Guidance for RSTs operating during a HD mission is described in Joint Guide (JG) 1-05, *Religious Affairs in Joint Operations*. In addition, RSTs will ensure they understand and adhere to all echelons of guidance, such as Service policy and doctrine, command direction, and legal counsel, regarding permissible chaplain activities. Upon the assessment and direction of the unit commander, RSTs may receive additional RS duties to assist other commands. The primary role and mission of the RST during HD is to support authorized personnel. However, RSTs may provide RS to persons unaffiliated with the Services absent other RS providers, and with proper command authority and tasking, consistent with the guidelines in JG 1-05, *Religious Affairs in Joint Operations.*

See JG 1-05, Religious Affairs in Joint Operations, *for details.*

g. **Joint Health Services.** The objective of health services is to provide lifesaving measures, as well as prevention, protection, and treatment capabilities, to mitigate the risk of disease nonbattle injuries, and battle injuries to support mission accomplishment. Joint health service provides joint medical capabilities to ensure the seamless delivery of medical support for military forces.

(1) DOD coordinates, employs, and integrates medical response through the capabilities of care: first responder care, forward resuscitative care, theater hospitalization, and definitive care.

(2) As part of planning activities and prior to deployment to an HD event, commands should conduct predeployment health assessments to ensure medical and dental requirements are current. Specific activities concerning exams, predeployment sample collections, issuance of medications, training on equipment and devices (e.g., respirator fittings), and record-keeping should be assessed.

(3) DOD medical assets and organizations may also be involved in support to local and state health providers in dealing with the aftermath of a CBRN attack and other large-scale, casualty-producing attacks. As part of HD, there may be a requirement to augment civilian medical capabilities in the handling of casualties resulting from CBRN attacks or other toxic materials release. The ability of state and local medical facilities to

handle mass casualties from CBRN effects must be assessed and factored into DOD planning.

For additional information, see JP 3-28, Defense Support of Civil Authorities, *and JP 4-02,* Joint Health Services.

9. Other Activities and Efforts

a. **Arctic Region.** The overarching strategic national security objective in the Arctic is a stable and secure region where US national interests are safeguarded and the US homeland is protected. This objective is consistent with current international law and diplomatic engagement, but also with demonstrated ability and commitment to defend the northern approaches to North America.

(1) DOD takes steps to anticipate and prepare for Arctic operations. Capabilities are reevaluated as conditions change, and gaps are addressed in order to prepare for operations in a more accessible Arctic. Key challenges include shortfalls in ice and weather reporting and forecasting, limitations in C2, communications, computer connectivity, intelligence, harsh environmental conditions, limited inventory of ice-capable vessels, and limited shore-based infrastructure. The US has a vital Arctic neighbor and partner in Canada, with its shared values and interests in the region. DOD works with the Canadian Department of National Defence to ensure common Arctic interests are addressed in a complementary manner.

(2) There are two GCCs with Arctic responsibilities: CDRUSEUCOM and CDRUSNORTHCOM are each responsible for a portion of the Arctic Ocean aligned with adjacent land boundaries—an arrangement suited to achieve unity of effort with key regional partners.

b. **Information Sharing**

(1) The objective of information sharing is to achieve seamless access to a trusted information sharing environment throughout the AOR and between CCDRs. A collaborative environment among domestic and international military and nonmilitary (i.e., LEA) HD mission partners is particularly critical 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 in support of HD, thereby 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 targets.

(2) Proper organization of the battle staff support structure is another way to synchronize and share information. In an adaptive HQ model, for example, the staff reorganizes from its normal functional areas of personnel, intelligence, operations, logistics, plans, and communications to working groups that address current operations, future operations, joint plans, joint support, and interorganizational coordination. The organization must also transcend culture, policy, and technical barriers to be effective.

Intentionally Blank

APPENDIX A
RELATIONSHIPS BETWEEN HOMELAND SECURITY, HOMELAND DEFENSE, AND DEFENSE SUPPORT OF CIVIL AUTHORITIES

1. General

a. **Achieving Unity of Effort Through HS, HD, and DSCA.** Perhaps one of the greatest challenges for a military staff is conducting military operations in or near the homeland that integrate into the overall USG unity of effort to secure and defend the homeland. This effort entails USG departments or agencies inherent authorities and jurisdiction at the federal, state, and local level, which DOD may support directly by providing forces or capabilities to HS operations, through DSCA, or if the magnitude of threat exceeds the capabilities of the HS enterprise, through HD operations. These TMM challenges are set against the evolving range of threats to the homeland, countering diverse threat networks, transregional terrorist organizations, potential nation state, and individual threats both internal and external to the US. This appendix provides additional context and considerations for the JFC and military staffs that plan and execute HD and DSCA missions, or otherwise directly support HS. Figure A-1 depicts the relationship between HD, DSCA, and HS missions and provides examples of the types of operations that can take place for each mission. Those missions could be conducted in a simultaneous, near-simultaneous, or sequential fashion, across the threat spectrum, within or near the homeland. A full range of threats and hazards confronts the homeland. However, many threats may not require a DOD-led response and may only require a response from one or more USG departments or agencies. Depending on the type of threat and its magnitude, the lead and supporting relationships may vary across the specific types of operations that can take place for each mission. HD, DSCA, and HS operations may occur in parallel and require extensive synchronization.

(1) **Threat Characterization.** The characterization of a particular threat, and the designated response agencies and modes, ultimately rests with the President. To prepare for wide-ranging contingencies, the USG has developed specific protocols and response options that address the coordination, integration, and responsibilities of the USG departments and agencies to respond to the full spectrum of threats and hazards. Codification of these strategies, processes, and procedures is found in documents such as the *National Strategy for Maritime Security* and *US Aviation Security Policy* and their respective supporting plans. These types of processes aid both the military and civil authorities to identify the organizations best suited to achieve the USG's desired outcome, given the unique circumstances of the event.

(2) **Transitioning Between HD, DSCA, and HS.** In addition, operations may also transition from HD to DSCA to HS or vice versa (e.g., maritime security) with the lead depending on the situation and USG's desired outcome (as depicted in Figure A-1). While the lead may transition, a single agency will always have the lead at any given time for a particular activity. However, in the areas of overlapping responsibility, the designation of LFA 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, which can transition between

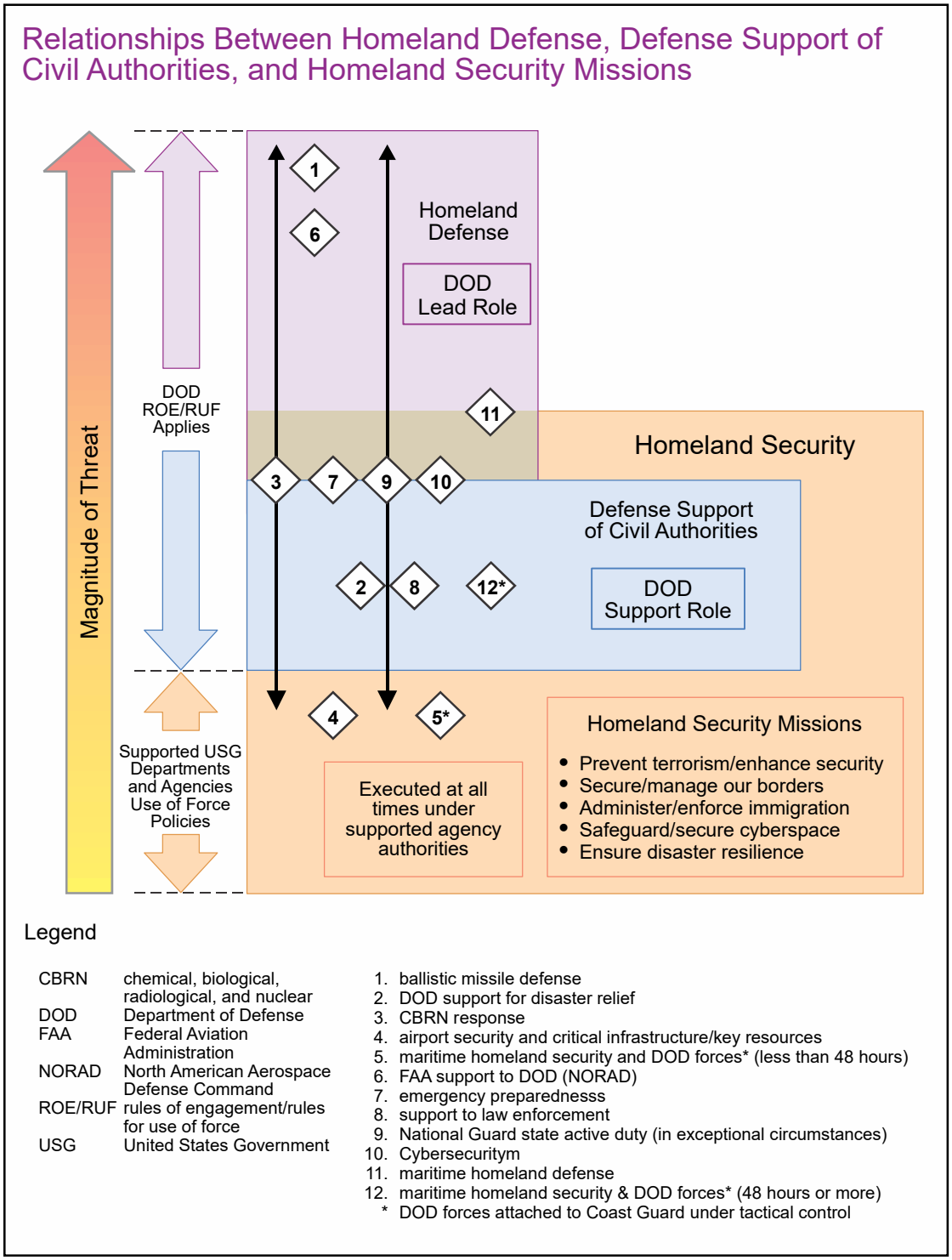


Figure A-1. Relationships Between Homeland Defense, Defense Support of Civil Authorities, and Homeland Security Missions

HD, DSCA, and HS (see Chapter III, "Planning and Operations for Homeland Defense"). The NG and the reserves also play a vital role in the defense of the homeland. Figure A-1 depicts NG Title 10, USC, authorities for HD and DSCA under DOD C2. It also depicts

NG Title 32, USC, authorities for HS, HD activities, and DSCA. Figure A-1 also depicts the fact that, in exceptional circumstances, NG forces may perform HD activities in state active duty. Title 32, USC, and state active duty fall under state or territory C2. EP remains part of DOD's overall preparedness activities. It spans HD, DSCA, 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. HD efforts often complement HS efforts and the reverse is also true.

b. **Key Departmental Roles**

(1) **DHS.** As stated in Chapter I, "Fundamentals of Homeland Defense," DHS, through DHS missions set forth in the Quadrennial Homeland Security Review, leads the HS enterprise in whole-of-government and community-based efforts to achieve HS. The *National Strategy for Homeland Security* addresses the terrorist threat and provides a comprehensive framework for organizing the efforts of federal, state, local, tribal, and private organizations whose primary functions are often unrelated to national security.

(2) **DOJ.** DOJ has lead responsibility for criminal investigations of terrorist acts or terrorist threats by individuals or groups inside the US, or directed at US citizens or institutions abroad, where such acts are within federal criminal jurisdiction of the US. They also have lead responsibility for related intelligence collection activities within the US, subject to the National Security Act of 1947 and other applicable law.

(3) **DOD.** DOD is a key part of the HS enterprise that protects the homeland through two distinct but interrelated missions, HD and DSCA. DOD is the federal agency with lead responsibility for HD, which may be executed by DOD alone (e.g., BMD) or include support from other USG departments and agencies. DOD's role in the DSCA mission consists of support of US civil authorities (DHS or other USG departments or agencies), as well as state, local, or tribal entities for domestic emergencies and for designated LE and other activities. While these missions are distinct, some department roles and responsibilities overlap and operations require extensive coordination between lead and supporting agencies. HD and DSCA operations may occur in parallel and require extensive integration and synchronization with HS operations. Understanding the roles and responsibilities of AC and RC forces and how they are used and the various duty statuses used to employ NG forces (Title 10 and Title 32, USC, and state active duty) is critical to achieve integration and synchronization.

2. Command and Control Options for Transition

a. In DOD, integration includes the synchronized transfer of units into an operational commander's force prior to mission execution. HD operations require special attention regarding integration, since the C2 possibilities are extensive. Traditional considerations for integration are generally 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, C2 becomes more complex. To promote seamless and interoperable interagency communications for the DSCA portion

of DOD missions, DODI 6055.17, *DOD Emergency Management (IEM) Program,* directs that DOD installations will adopt and implement procedures consistent with the National Incident Management System (NIMS). Procedures will include a well-defined communication plan that includes the capability to communicate within DOD, with personnel conducting the response, as well as with civil authorities. For interoperability, the Incident Command System per the NIMS will be used in the civil sector. This approach provides for common interaction when DOD is in support of civil authorities and requires planning consideration by the JFC performing such dual mission sets.

b. CCDRs cannot predict when an HD operation will transition to DSCA or vice versa. Additionally, CCDRs may need to execute HD and DSCA simultaneously. Thus, C2 in support of HD and DSCA operations should have a straightforward C2 template that permits the CCDR to respond as the supported commander, supporting commander, or both. Changes in law and DOD policy have increased the CCDR's C2 options. Options include using a standing JTF HQ, augmenting a core Service component HQ, or forming an ad hoc organization from various contributors. Regardless of the organizational structure, there are fundamental rules for forming and operating a JTF.

3. Planning Considerations for Transition

a. **Employment of RC Forces.** The RC possesses resources (personnel, equipment, and skills) that can be appropriately leveraged and effectively integrated into DOD's HD plans and operations, based on the operational requirements. When mobilized, RC forces operate as active duty forces. While the NG is normally 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. When placed on federal active duty, all RC forces conduct HD operations under Title 10, USC, guidelines.

b. **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. Latitude and longitude values can be based on different geodetic systems, or datums. The most common is the World Geodetic System 1984, a global datum used by all Global Positioning System equipment. Other datums are significant because they were chosen by a cartographical organization as the best method for representing their region and are used on printed maps and charts. The latitude and longitude on a printed map or chart may not be the same as the Global Positioning System receiver. Coordinates from the mapping system can sometimes be roughly changed into another datum using a translation. This need for translation may complicate coordinating activities between federal, state, tribal, and local responders.

c. **USCG.** The USCG has inherent authorities and capability to seamlessly transition between HS and HD operations. As discussed in Chapter II, "Command Relationships and Interorganizationl Cooperation," USCG execution of MHD tasks will be under the C2 of CGDEFOR, and USCG execution of MHS tasks will be under the C2 of USCG commanders. Additional considerations for the transition of USCG operations between MHS and MHD include the following:

(1) **Ports, Waterways, and Coastal Security (PWCS).** In general, the USCG PWCS mission under the regime of MHS overlaps with many MHD port security and harbor defense activities. It is important for JFC planning purposes to note that MHS operations are always in effect, and there are significant force demands within the USCG to conduct MHS, especially if maritime security conditions increase in a heightened threat environment. The USCG may also raise maritime security condition levels, which generally increases vessel and port security activities at the federal, state, and local levels and across commercial enterprise within the maritime transportation system and may lead to USCG force requirements for DOD to support MHS. A particular advantage of PWCS over MHD port security and harbor defense activities is the more flexible USCG use of force policy, compared to more restrictive SROE. Only in circumstances where SROE is necessary to defeat a particular threat should a transition from PWCS to MHD be considered.

For more information on PWCS activities in relation to USCG-declared maritime security conditions, see COMDTINST M16600.6, Maritime Security and Response Operations (MSRO) Manual.

(2) **COTP Functions.** The USCG's regulatory functions are also a key planning factor for JFC staffs planning maritime operations in areas subject to US jurisdiction. Both the Magnuson Act and Port Waterways Safety Act grant regulatory powers to the USCG Commandant and the various designated COTPs. JFC staffs may coordinate regularly with USCG staffs to identify pre-planned regulatory actions, including safety and security zones that may be required to support joint MHD operations.

For more information on COTP functions, see Title 33, Code of Federal Regulations, Parts 6 and 165, *and COMDTINST M16000.11,* Marine Safety Manual, Volume VI, Ports and Waterways Activities.

(3) **Balancing Enforcement and Security with Defense.** The USCG conducts LE operations and joint MIO using cutter and shore based boarding teams, LE detachments, and maritime security response team direct action sections, as needed. The USCG will normally require DOD-provided lift and surface assets under the auspices of direct MHS support if USCG cutters or aircraft are unavailable to support short-notice maritime response operations. When necessary, USCG assets conduct operations that preserve evidence required for prosecution of a maritime threat under US law while balancing risk associated with certain types of boarding operations. As a member of the IC, the USCG may also contribute to tactical intelligence exploitation in support of other federal agencies when such activities are authorized by US law and policy.

For more information, see COMDTINST M16247.1, Maritime Law Enforcement Manual (MLEM); *COMDTINST M16600.6,* Maritime Security and Response Operations (MSRO) Manual; *and Coast Guard Publication 3-2,* Short Notice Maritime Response.

(4) **Domestic MHS Coordination.** Maritime security authorities that contribute to both HS and HD include domestic frameworks that coordinate partnerships, establish maritime security standards, collaborate with shared maritime security interests, and

facilitate the sharing of information. Domestically, the USCG-led area maritime security committees carry out much of the maritime security regime effort. COTPs, in their role as federal maritime security coordinator, lead the area maritime security committees through state-wide and municipal-level coordination with federal, state, and local LEAs and commercial port partners. In exercising COTP authority, COTPs consider all equities in the port environment as certain regulatory actions can have significant economic impact and may dictate trade-offs with security demands.

(5) **International MHS Activities.** Abroad, and in a similar fashion to how DOD conducts defensive activities in the forward regions whenever possible, the USCG conducts the International Port Security Program, which works with other countries and through the International Maritime Organization, a specialized agency of the United Nations.

For more information on USCG domestic and international port security compliance, see COMDTINST M16000.12, Port Security Compliance Manual.

d. **Auxiliary Organizations**

(1) **USAF Auxiliary.** The USAF 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 USAF IAW Title 10, USC, Section 9442, to support USAF noncombat programs and missions. Such missions may include 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.

(2) **USCG Auxiliary.** The USCG Auxiliary was established by Congress in 1939 under Title 14, USC. The USCG Auxiliary supports MHS through the USCG Port Safety and Security Program. For more information, see COMDTINST M16790.1, *Auxiliary Manual.*

(3) **Military Auxiliary Radio System.** Both the USA and the USAF maintain auxiliary communications that can handle unclassified message traffic, including encryption capabilities.

e. **State Defense Forces.** State defense forces (e.g., state military, state guards, or state military reserves) are military units that operate under the sole authority of a state government; they are partially regulated by the NGB but they are not a part of the ARNG. State defense forces are authorized by state and federal law and are under the command of the governor of each state. There are active state defense forces in 20 states and the US territory of Puerto Rico. At the discretion of individual states or territories, state defense forces may support, assist, and augment their state's NG forces and civilian authorities such as police and fire departments.

f. **Chapter 18 (Title 10, USC, Sections 271-282).** This chapter concerns military support for civilian LEAs and provides statutory authority for specific types of military

support to LE. Title 10, USC, Section 275, 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 DODI 3025.21, *Defense Support of Civilian Law Enforcement Agencies.*

g. **Insurrection (Title 10, USC, Sections 251-255).** These statutory provisions allow the President, at the request of a state governor or legislature, or unilaterally in some circumstances, to employ the US Armed Forces to suppress insurrection against state authority, to enforce federal laws, or to suppress rebellion. When support is directed for such HD-related purposes in the US, the designated JFC should utilize this special application knowing the main purpose of such employment is to help restore law and order with minimal harm to the people and property and with due respect for all law-abiding citizens.

h. **CIP.** 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 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 the homeland. These will include DCI assets and DIB assets, the protection of which is the responsibility of DOD. JFCs' preparations to conduct CIP should consider those in either a HD or DSCA role or as one transitions from one to another. For example, an explosion occurs at a major dam or nuclear facility. These are considered key assets from a national perspective. With no initial determination of cause, authorities suspect terrorism. National leadership makes the initial determination to deploy a QRF for HD to protect critical infrastructure due to unknown intent and for the purpose of expediency. Subsequent to QRF arrival, an assessment is made whether an external threat or terrorism caused the event. Upon such determination of threat, but if a need for security remains, the QRF would perform security in a DSCA role until sufficient numbers of other federal agency, local LE, and/or NG (Title 32, USC) can provide necessary support.

For complete details on the DSCA mission, see JP 3-28, Defense Support of Civil Authorities.

Intentionally Blank

APPENDIX B
FACILITATING INTERORGANIZATIONAL COOPERATION

1. General

DOD leads HD missions and will be supported by other USG departments and agencies while conducting such missions. Conversely, DOD supports other USG departments and agencies for DSCA missions. Events or operations that begin as HD missions may transition to a DSCA mission (normally for response to an incident) or evolve to a concurrent DSCA mission. This appendix identifies organizations that normally support HD missions in some fashion, notwithstanding that some may also support DSCA missions separately, concurrently, or as a follow-on requirement.

2. Combat Support Agencies and Other Supporting Organizations

CSAs provide direct support to the CCMDs performing HD during wartime or emergency situations and are subject to evaluation by the CJCS. The paragraphs below address general and specific missions, functions, and capabilities of DOD CSAs and other selected organizations which conduct HD activities.

a. **DISA.** DISA provides, operates, and assures C2, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national-level leaders, and other mission and coalition partners. DISA supports national security communications requirements and functions within the following core mission areas: communications; C2 capabilities; cybersecurity; computing services; interoperability, testing, and standards; DODIN services; engineering; and acquisition. It is the Defense Infrastructure Sector Lead Agent for the DODINs, per DODD 3020.40, *Mission Assurance (MA),* and implements and executes the DCIP requirements. Joint Force HQ-DODIN, a staff subordinate to CDRUSCYBERCOM, plans, directs, coordinates, integrates, and synchronizes execution of global DODIN operations and DCO internal defensive measures to secure, operate, and defend the DODIN.

For more information on DISA, see DODD 5105.19, Defense Information Systems Agency (DISA).

b. **DIA.** DIA provides intelligence on foreign militaries and operating environments that delivers decision advantage to prevent and decisively win wars. The Director of DIA advises SecDef and the Deputy Secretary of Defense, CJCS, CCDRs, and Under Secretary of Defense for Intelligence on all matters concerning military and military-related intelligence and is the principal DOD intelligence representative in the national foreign intelligence process.

For more information on DIA, see DODD 5105.21, Defense Intelligence Agency (DIA). *See also JP 2-0,* Joint Intelligence.

c. **DLA.** DLA provides worldwide logistics support for the missions of the Military Departments and the CCMDs. Specifically:

(1) DLA provides support to other DOD components and USG departments and agencies, and, when authorized by law, state and local government organizations, foreign governments, and international organizations.

(2) DLA provides support to USNORTHCOM and USPACOM for planning and execution of HD. DLA has many capabilities in USPACOM's AOR led by the DLA-Pacific Regional Command. DLA has LNOs positioned at USNORTHCOM that can be augmented during a crisis. An operational planning team is located at DLA HQ, with planners dedicated to each CCMD. A catalog of DLA-type unit capabilities is available to both commands for planning and execution in the Adaptive Planning and Execution system. The Defense Logistics Agency support team, a type unit capability, that when deployed/employed in a JOA, is the primary focal point for disseminating, coordinating, and tracking issues of the CCDR or JFC concerning DLA.

(3) Provides enabler OCS support to CCDR planning efforts and training events and, when requested, advises, assists, and JFC oversight of OCS during HD and DSCA operations.

For more information on DLA, see DODD 5105.22, Defense Logistics Agency (DLA), *and JP 4-0,* Joint Logistics.

d. **National Security Agency (NSA).** NSA provides the following support:

(1) Solutions, products, and services that contribute to cybersecurity.

(2) SIGINT for an effective, unified organization and control of all the foreign signals collection and processing activities of the US. NSA is authorized to produce SIGINT IAW objectives, requirements, and priorities established by the Director of National Intelligence with the advice of the National Foreign Intelligence Board.

(3) Information systems security activities, as assigned by SecDef, to include managing and providing OPCON of the US SIGINT System.

For more information on the responsibilities of NSA, refer to EO 12333, United States Intelligence Activities.

e. **Defense Contract Management Agency (DCMA).** DCMA works directly with defense suppliers to help ensure DOD, USG, 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 DIB sector.

f. **National Geospatial-Intelligence Agency (NGA).** 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. GEOINT consists of imagery, imagery intelligence, and geospatial information. NGA also:

(1) Supports customers in the defense, LE, 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 provide a common frame of reference for USG decision makers and operational planners regarding critical infrastructure vulnerability analysis, domestic incident management, and CIP.

(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, incident management, 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 National Geospatial-Intelligence Agency support team (NST) program to CCMDs, the Services, IC partners, and USG departments and agencies (e.g., DOS, FBI, and DHS). These embedded NST personnel provide day-to-day GEOINT support to the commands or agencies and have the capability to reach back to NGA for requirements that exceed the capacity or capability of the team. In addition, NGA maintains a group of support personnel as part of NGA voluntary deployment teams that can deploy to augment an NST. NST members or individuals from the NGA voluntary deployment teams can be called upon to participate as part of a national intelligence support team, along with other members of the IC, in response to a crisis or emergency situation to augment the staffs of a JIOC, command, or agency.

g. **DTRA.** DTRA's mission is to safeguard the US and its allies from global WMD and improvised threats by integrating, synchronizing, and providing expertise, technologies, and capabilities. DTRA provides integrated technical and operational solutions, as well as intellectual capital, to inform and support national-level and DOD policies and strategies that address WMD and improvised threats to the homeland and the warfighter. Additionally, DTRA provides support to DOD components, interagency stakeholders, and allied partners to ensure a safe, secure, reliable, and effective strategic nuclear deterrent for defense of the homeland. Specific DTRA capabilities that help prevent acquisition of WMD and related materials, contain and reduce threats, and respond to crisis in defense of the homeland include the following functions:

(1) Provide continuous support to the warfighter through its National CWMD Technical Reachback Enterprise, a national CWMD support element that provides CWMD analysis and decision support capability for planning, operations, and post-event analysis to CCMDs, the Office of the Secretary of Defense, the JCS, the IC, DOD command elements, other USG departments and agencies, and first responders.

(2) Balanced survivability assessments are mission survivability assessments of critical national or theater mission systems, networks, architectures, infrastructures, and assets of the US and its multinational partners. Assessment areas include surveillance operations; physical security; telecommunications; selected information-related capabilities; DCO; and cyber security analysis, structural protection and response, utility subsystems, WMD protection, emergency operations, and electromagnetic protection.

(3) CBRN military advisory teams, when requested, provide technical and scientific subject matter experts, planners, and hazard prediction modeling support to CCDRs and federal coordinating agencies or their delegated representatives in response to catastrophic incidents involving WMD in the US and abroad.

(4) Deployable CWMD plans teams assist CCMDs or other supported commanders with CWMD planning and analysis of existing plans or assist the supported commander in developing plans, annexes, or appendices for CWMD operations.

(5) The mission assurance methodology integrates 10 protection programs (AT, DCI, COOP, emergency management, LE, FHP, defense security enterprise, fire prevention and protection, insider threat, and cybersecurity) into a single risk assessment process with common standards and metrics ensuring commanders at all levels are more informed as to the overall risk to mission. A joint mission assurance assessment is a "risk-based" assessment of an installation's ability to mitigate threats from all hazards and threats. A risk-based assessment addresses the impact to missions if affected by an identified hazard or threat.

(6) Technical support groups located in CONUS, USPACOM, United States European Command (USEUCOM), US Africa Command, and US Central Command provide the capability to train, advise, assist, and equip in order to conduct tactical low-visibility radiological search operations.

(7) DTRA serves as DOD lead for US nuclear weapon incident training and executes the Nuclear Weapon Accident Incident Exercise program along with supporting training events.

(8) DTRA's Joint Improvised-Threat Defeat Organization (JIDO) enables DOD actions to counter improvised threats through anticipatory and rapid acquisition and with tactical responsiveness in support of CCDRs' efforts to prepare for, and adapt to, battlefield surprise in support of CT, counterinsurgency, and other related mission areas, including counter-improvised explosive devices. JIDO capabilities to enhance CCDR readiness to perform HD activities include:

(a) Enhanced situational understanding of improvised threats through a global common operational and intelligence picture.

(b) Forward-deployed and embedded presence at critical points in order to illuminate threat networks, their activities, and vulnerabilities.

(c) Peacetime, contingency, and crisis support that enables the pursuit of threat networks, their urgent and emerging use of technologies, and counter-threat requirements and solutions.

(d) Establishing and enabling communities of action to leverage the capabilities, authorities, and access of DOD, national laboratories, USG departments and agencies, industry, academia, and international partners to assist with counter-improvised threat solution development.

(e) Applying weapons technical intelligence tools and solutions for forensic and technical exploitation of asymmetric/improvised weapons.

(f) Expeditionary, quick reaction surge, and reachback support to enhance tactical and operational responsiveness to CCMD contingency operations.

(g) Threat and counter-threat intelligence, information, and capabilities in support of military and joint training programs.

(h) Supporting Military Departments/Services' predeployment training and CCMD's priority training exercise support.

For additional information on DTRA capabilities, see DODD 5105.62, Defense Threat Reduction Agency (DTRA).

h. **JIATF-S.** JIATF-S is a multi-Service, multiagency, national task force based at Naval Air Station Key West, Florida. JIATF-S detects and monitors aircraft and maritime vessels suspected of trafficking in illicit goods and then provides this information to international and interagency partners who have the authority to interdict illicit shipments and arrest members of TCOs. In support of HD, JIATF-S helps track military equipment destined for terrorist organizations. The interorganizational cooperation that occurs daily promotes shared responsibilities and facilitates appropriate and legal LE information sharing between non-DOD LEAs (both US and other countries). This, and the combined operations that are conducted under JIATF-S auspices, supports a concerted HD and HS approach to protecting US national interests in Latin America and the Caribbean.

i. **JIATF-W.** JIATF-W is the USPACOM Executive Agent for DOD support to LE for CD and drug-related activities. The JIATF-W team is a composite of active duty, reserve, DOD civilian, contractor, and US and foreign LEA personnel. JIATF-W plans, integrates, synchronizes, conducts, and assesses DOD CD activities for CDRUSPACOM in order to shape the theater and disrupt TCOs that threaten US interests in the USPACOM AOR. JIATF-W targets organizations that threaten the US, its territories, and its interests so they are denied the ability to traffic illicit drugs and precursor chemicals used to produce

illicit drugs in the USPACOM AOR; the OE is less permissive for their activities, and regional partnerships and stability are enhanced.

j. **Missile Defense Agency (MDA).** The MDA is a research, development, and acquisition agency within DOD whose mission is to develop and deploy a layered BMD system to defend the US, deployed forces, allies, and friends from ballistic missile attacks from all ranges in all phases of flight. This includes using international cooperation by supporting mutual security interests in missile defense. The agency works with the CCDRs (e.g., USNORTHCOM, USPACOM, and USSTRATCOM) to develop BMD systems technologies and a program to address the challenges of an evolving threat. The agency uses the Missile Defense Integration and Operations Center (MDIOC) as the central communications node for situation monitoring and information collection on current BMD systems performance. From the MDIOC, MDA can coordinate support to the CCDRs, Services, and other agencies and provide staff assistance to BMD systems element managers. The MDIOC functions include the coordination and monitoring of concurrent operational and test activities of the BMD systems, supporting emergency activation of BMD system test bed resources for operational execution, and for receiving and disseminating New Strategic Arms Reduction Treaty and Treaty on Open Skies inspection information. MDA also supports BMD systems asset management and logistical support. Asset management enables event owners and asset owners to deconflict their events and asset requirements (e.g., tests and maintenance) and to use a cooperative approach between CCDRs, Services, and MDA to provide for the capability testing, sustainability, and maintainability of MDA elements and components.

k. **Department of Defense Cyber Crime Center (DC3).** DC3 provides digital forensics support to DOD and to other LEAs. The DC3's main focus is in criminal, CI, CT, and fraud investigations, but two of the groups associated with the DC3 support HD-related efforts. These are the DOD-Defense Industrial Base Collaborative Information Sharing Environment (DCISE), National Cyber Investigative Joint Task Force-Analytical Group (NCIJTF-AG), and Defense Cyber Investigations Training Academy.

(1) DCISE is the focal point and clearinghouse for referrals of intrusion events on DIB unclassified corporate networks. The DCISE is a collaborative information sharing environment among multiple partners that produces threat information products for industry partners with reciprocal responsibilities of providing notice of anomalies and sharing of relevant media.

(2) The NCIJTF-AG coordinates with the National Cyber Investigative Joint Task Force, a cyberspace investigation coordination organization overseen by the FBI which serves as a multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyberspace threat investigations. The NCIJTF-AG mitigates, neutralizes, and disrupts cyberspace intrusions presenting a national security threat. The NCIJTF-AG synthesizes a COP of hostile intrusion related activity to aid investigations, review all source data, and support timely reporting in order to shrink the cyberspace CI response time on defense-related intrusions.

l. **Defense Forensics and Biometrics Agency (DFBA).** DFBA leads, consolidates, and coordinates forensics and biometrics activities and operations for DOD in support of identity activities.

(1) DFBA operates DOD's authoritative biometrics repository, the Automated Biometric Information System, collected on foreign nationals throughout the course of military operations and shared by PNs and interagency partners. DFBA's efforts provides significant contribution to the whole-of-government CT approach to collect, match, store, share, and use biometrics to the fullest extent practicable, lawful, and necessary to protect national security interests.

(2) DFBA performs the dissemination of the DOD Biometric Enabled Watch List on behalf of DIA and provides the conduit for matching against interagency authoritative data sets (DHS's IDENT [Automated Biometric Identification System] and the FBI's NGI [Next Generation Identification] databases).

3. Other United States Government Departments and Agencies

a. **DHS.** Key directorates and components of DHS, as they relate to HD, include:

(1) **The Science and Technology Directorate** is the primary research and development arm of DHS. The Science and Technology Directorate provides federal, state, and local officials with the technology and capabilities to protect the homeland.

(2) **The National Protection and Programs Directorate** 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 US borders, seaports, bridges and highways, and critical information systems. The directorate has five divisions: Federal Protective Services, CS&C, Office of Infrastructure Protection, Office of Risk Management and Analysis, and United States Visitor and Immigrant Status Indicator Technology (biometrics-based technological solutions).

(3) **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.

(4) **The Office of Health Affairs** is DHS's principal authority for all medical and health issues. This office anticipates the public health impact of biological attacks, chemical releases, pandemics and infectious disease threats, and disasters to help prepare the nation to respond and rebound.

(5) **The Office of Partnership and Engagement** coordinates DHS's outreach efforts with critical stakeholders nationwide, including state, local, tribal, and territorial governments; elected officials; LE; the private sector; and colleges and universities, ensuring a unified approach to external engagement. This office advocates and represents

interests of these stakeholders through DHS's policy making process and as a conduit for the Secretary of Homeland Security to engage with stakeholders or share information.

(6) **The Office of Intelligence and Analysis** uses information and intelligence from multiple sources to identify and assess current and future threats to the US.

(7) **The Operations Coordination and Planning Directorate** monitors the security of the US on a daily basis and coordinates activities within DHS and with governors, advisors, LE partners, and critical infrastructure operators' areas nationwide.

(8) **The Domestic Nuclear Detection Office** 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. It is the primary entity in the USG for implementing domestic nuclear detection efforts for a managed and coordinated response to radiological and nuclear threats, as well as the integration of federal nuclear forensics programs. This office coordinates the development of the global nuclear detection and reporting architecture, with partners from federal, state, local, and international governments and the private sector.

(9) **The Federal LE Training Center** serves as an interagency LE training organization for 91 federal agencies. It also provides services to state, local, tribal, and international LEAs.

(10) **US Customs and Border Protection** protects the nation's borders to prevent terrorists and terrorist weapons from entering the US. It facilitates the flow of legitimate trade and travel while enforcing US regulations, including immigration and drug laws.

(11) **US Citizenship and Immigration Services** is the USG agency that oversees lawful immigration to the US. It administers immigration and naturalization adjudication functions and establishes immigration services policies and priorities.

(12) The **USCG** is one of the five military Services under Title 10, USC, and established separately within DHS under Title 14, USC.

(13) **FEMA** supports US citizens and first responders to ensure, as a nation, we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards.

(14) **US Immigration and Customs Enforcement** promotes HS and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration. It identifies and shuts down vulnerabilities on the nation's border and in the economic, transportation, and infrastructure security.

(15) **The US Secret Service** mission is to safeguard the nation's financial infrastructure and payment systems to preserve the integrity of the economy and to protect the President and other national leaders, visiting heads of state and government, designated

sites, and national special security events. The US Secret Service's partnerships—public and private, domestic and international, LE and civilian—play a critical role in preventing, detecting, investigating, and mitigating the effects of electronic and financial crimes.

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

For additional information on DHS directorates and offices, refer to JP 3-08, Interorganizational Cooperation.

b. **DOJ/FBI.** As the lead for crisis management and CT, the Attorney General investigates terrorist acts or threats; coordinates LE activities to detect, prevent, preempt, and disrupt terrorist attacks; and, if an attack occurs, to identify and prosecute the perpetrators. The FBI, as LFA, manages the federal LE 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. The FBI maintains two operational watches within a single operations center, the Strategic Information and Operations Center (SIOC) Watch and CT Watch. The SIOC Watch retains primary daily responsibility for criminal investigative matters, administrative issues, and information management. The CT Watch works side-by-side with the SIOC Watch to support seamless and efficient handling of strategic information and emerging events, both domestically and globally. The dual location of both watches supports the proper flow of information to FBI HQ, field divisions, legal attachés, and other government agency operations centers within the IC. The Crisis Coordination and Administration Unit within the SIOC coordinates and prepares the operational activation system at FBI HQ for a watch, threat or incident, special event, or natural disaster. This includes coordination with field offices, legal attachés, and specialized national assets when required to manage a critical incident. Additionally, the SIOC supports FBI field commanders who represent the FBI worldwide in major investigations, tactical operations, and other matters.

c. **DOE.** DOE/National Nuclear Security Administration is the USG's primary capability for radiological and nuclear emergency response and for providing security to the nation from nuclear terrorism. DOE maintains a high level of readiness for protecting and serving the US and its multinational partners through the development, implementation, and coordination of programs and systems designed to respond in the event of a nuclear terrorist incident or other types of radiological accidents. DOE provides a dedicated resource capable of responding rapidly to nuclear or radiological incidents worldwide. Key areas include radiological search teams to locate and identify radiological material, render safe capability to make sure a nuclear device is safe, and CBRN response to determine the spread of radiological material.

(1) DOE also has a variety of emergency response assets. These assets encompass four core competencies: core knowledge of US nuclear weapons, "dirty bombs," and crude nuclear devices; core knowledge of use and interpretation of specialized radiation detection equipment; core technical operations; and core technical support requirements.

(2) The assets are:

(a) **Aerial Measuring System.** The Aerial Measuring System utilizes aerial platforms to characterize ground-deposited radiation. These platforms include fixed-wing and rotary-wing aircraft with radiological measuring equipment; computer analysis of aerial measurements; and equipment to locate lost radioactive sources, conduct aerial surveys, or map large areas of contamination.

(b) **Accident Response Group.** The Accident Response Group response element is comprised of scientists, technical specialists, crisis managers, and equipment ready for short-notice dispatch to the scene of a US nuclear weapon accident.

(c) **National Atmospheric Release Advisory Center.** The National Atmospheric Release Advisory Center is a computer-based EP and response predictive capability. It provides real-time computer predictions of the atmospheric transport of material from radioactive release.

(d) **Federal Radiological Monitoring and Assessment Center.** The Federal Radiological Monitoring and Assessment Center is a federal asset available on request by DHS and state and local agencies to respond to a nuclear or radiological incident. This organization has representation from the National Nuclear Security Administration, DOD, the Environmental Protection Agency, the Department of Health and Human Services (DHHS), the FBI, and other USG departments and agencies.

(e) **Radiological Assistance Program.** The Radiological Assistance Program also provides advice and radiological assistance for incidents involving radioactive materials that pose a threat to the public health and safety of the environment. It can provide field deployable teams of health physics professionals equipped to conduct radiological search, monitoring, and assessment activities.

(f) **Radiation Emergency Assistance Center/Training Site.** This site provides medical advice, specialized training, and onsite assistance for the treatment of radiation exposure accidents.

(g) **Nuclear Emergency Support Team (NEST).** NEST provides technical assistance to a LFA to deal with nuclear threats and incidents. NEST addresses threats by domestic and foreign terrorists that may have the will and means to employ WMD. NEST assists in the identification, characterization, rendering safe, and final disposition of any nuclear weapon or radioactive device.

d. **DOT/FAA.** The mission of DOT is to ensure a fast, safe, efficient, accessible, and convenient transportation system that meets US vital national interests and enhances the quality of life of the American people. Under DOT, the FAA provides air movement and flight plan data for all aircraft operations. It 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, the FAA clears air traffic as needed 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 rates and certifies airmen and 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 which perform 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 (ADSs). These and other support activities and procedures are governed by a series of agreements and FAA orders.

e. **NCTC.** The NCTC is organizationally part of the Office of the Director of National Intelligence and is staffed by more than 16 departments and agencies. NCTC has two core missions. The first is to serve as the primary organization in the USG for analysis and integration of all terrorism intelligence and, in that capacity, the Director reports to the Director of National Intelligence. The second mission is to conduct strategic operational planning for CT activities integrating all elements of US national power. In this role, the Director reports to the President. The NCTC serves as the central and shared knowledge bank on terrorism information, provides all-source intelligence support to government-wide CT activities, and establishes the information technology systems and architectures within the NCTC and between the NCTC and other agencies that enable access to, as well as integration, dissemination, and use of, terrorism information. One way the NCTC supports HD is its operation of a secure website, NCTC Online CURRENT, which serves as the primary dissemination mechanism for terrorism information produced by the NCTC and other CT mission partners, to include international partners. NCTC Online CURRENT is directly available to a broad audience and includes USG partners with an operational focus (e.g., FBI's JTTFs and DOD's CCMDs).

f. **DHHS**

(1) **The Centers for Disease Control and Prevention (CDC).** The CDC is a USG agency under DHHS. It is the US's national-level public health institute and works to protect public health and safety by providing information to enhance health decisions, and it promotes health through partnerships with state health departments and other organizations.

(2) **The Public Health Emergency Medical Countermeasures Enterprise** coordinates federal efforts to enhance CBRN threats and emerging infectious diseases preparedness from a medical countermeasures perspective. It is led by the DHHS Office of the Assistant Secretary for Preparedness and Response and includes three primary DHHS internal agency partners: the CDC, the Food and Drug Administration, and the National Institutes of Health, as well as several interagency partners: DOD, the Department of Veterans Affairs, DHS, and the Department of Agriculture.

Intentionally Blank

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

"Mindful in the years since the first NORAD [North American Aerospace Defense Command] Agreement was concluded in May 12, 1958, NORAD, as a distinct command, has evolved to address the continuing changes in the nature of threats to North America and that it will need to adapt to future shared security interests."

***NORAD Agreement*, 2006**

1. North American Aerospace Defense Command Overview

a. Since 1957, Canada and the US have defended the skies of North America. A formal NORAD Agreement between the two governments was signed on 12 May 1958 to establish NORAD as a bi-national 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. 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.

b. As an executed international covenant, the NORAD Agreement is binding under international law. The 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, 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 GCC.

2. Missions

a. **Aerospace warning** consists of processing, assessing, and disseminating intelligence and information related to man-made objects in the air and space domains, plus 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 US commands that are responsible for missile defense.

b. **Aerospace control** consists of providing surveillance and exercising NORAD OPCON of the airspace of the US and Canada. NORAD OPCON is defined in the NORAD Agreement and NORAD Terms of Reference as the authority to direct, coordinate, and control the operational activities of forces assigned, attached, or otherwise made available to NORAD. Aerospace control involves a continuum of combined air operations that includes air sovereignty operations aimed at controlling access to the sovereign airspace of North America, air enforcement operations aimed at controlling activities approaching or within sovereign airspace, and air defense operations aimed at defending against air attack. This means NORAD has the authority to monitor, control, and prosecute (in cooperation with the FAA and Transport Canada/NAV CANADA) all unwanted and unauthorized activity approaching and/or operating within North American airspace, including cross-border air operations.

c. **Maritime warning** consists of processing, assessing, and disseminating intelligence and information related to the respective maritime approaches to the US and Canada. It also includes warning of maritime threats to, or attacks against, North America utilizing mutual support arrangements with other commands and agencies, to enable identification, validation, and response by national commanders and agencies responsible for maritime defense and security. These tasks develop a comprehensive shared understanding of maritime activities to better identify potential maritime threats to North American security. Maritime surveillance and control should be exercised by national commands and, as appropriate, coordinated bilaterally.

3. Supporting Mission Areas and Systems

a. **ITW/AA.** Tactical warning is a warning after initiation of a threatening or hostile act based on an evaluation of information from all available sources. Attack assessment is an evaluation of information to determine the potential or actual nature and objectives of an 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 IAW the priority assigned to attacks against North America.

b. **Routine Air Operations.** NORAD provides 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 US. 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 UA approaching North America.

(2) Air defense against manned or UA 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 US. A "need to share" philosophy facilitates the effective execution of these NORAD missions on behalf of the governments of Canada and the US.

d. **Interorganizational Cooperation.** The effective execution of NORAD missions requires significant cooperation with agencies outside the Department of National Defence in Canada and DOD in the US. 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. **Direct Communications.** CDRNORAD is authorized direct communications with the CDS; CJCS; SecDef; Commander, CJOC; CDRUSNORTHCOM; CDRUSPACOM; CDRUSSTRATCOM; CDRUSSOUTHCOM; nation Service chiefs; and other commanders on matters relative to NORAD's missions. This includes requests to appropriate agencies to expedite the release of classified information to facilitate the accomplishment of NORAD's missions.

f. **CD and Countering Transnational Organized Crime Operations.** TCOs facilitate 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 US by both governments. DOD is the LFA to detect and monitor illegal airborne and maritime drug trafficking into the US. To accomplish this mission, SecDef tasked CDRNORAD and selected CCDRs to support the GCCs planning and execution requirements for CD and to counter TCOs, required. Likewise, the Canadian National Drug Strategy named the National Defense Headquarters (Canada) as a supporting department to the Royal Canadian Mounted Police. As a result, 1 Canadian Air Division (CAD) is responsible for conducting CD operations when directed by National Defense Headquarters (Canada). 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

> *"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."*
>
> **Canada-United States Basic Defense Document**
> **July 2006**

detecting, monitoring, and apprehending aerial drug traffic; and integrates NORAD operations into an effective CD network.

For more information on the differences between Canadian and US law for military support to LEAs, refer to NORAD Instruction 10-24, (U) Counterdrug (CD)/Counter Narcoterrorism (CNT) Operations.

4. North American Aerospace Defense Command Organization

NORAD is organized on three distinct levels. The HQ NORAD staff and the command center operate at the strategic level. The three NORAD regions conduct activities at the operational level, and the ADSs and their TACON forces operate at the tactical level.

a. Missions are accomplished through a combination of assigned and attached Canadian and US forces (AC, NG, and reserves). These forces are employed in three NORAD regions, further described in paragraph 6, "North American Aerospace Defense Command Subordinate Commands."

b. **CDRNORAD.** CDRNORAD and the Deputy Commander cannot be from the same country, and their appointments must be approved by both Canadian and US governments. The jurisdiction of CDRNORAD over those forces specifically made available to NORAD by the two governments is limited to OPCON.

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

d. **HQ NORAD.** HQ NORAD provides the strategic guidance necessary for the regions to execute their assigned missions. Additionally, the HQ coordinates with the senior military staffs of both countries, as well as other CCDRs who may be in a supporting role. HQ NORAD and the command centers are composed of integrated staffs with representatives of both countries.

e. **HQ NORAD Staff Organization.** The HQ NORAD staff is organized along the same J-code construct as the Joint Staff. In addition, the commander's staff includes Canadian and US political advisors, an interagency group, a Washington Office, and special assistants for NG and reserve affairs. A unique aspect of the HQ NORAD staff is that most staff elements are dual-hatted as both NORAD and USNORTHCOM organizations. The exception is the operations directorate, which is a NORAD-only organization. Despite most of the staff being dual-hatted with USNORTHCOM, the commands remain separate with complementary missions, roles, and responsibilities.

5. North American Aerospace Defense Command Relations with Other Commands

a. **USNORTHCOM.** NORAD and USNORTHCOM share a special and unique relationship. A majority of USNORTHCOM's AOR and NORAD's OA overlap. 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 bi-national military organization which exists under the authority of the North Atlantic Treaty, the NORAD Agreement, the NORAD Terms of Reference, and the Canada-United States Basic Defense Document between Canada and the US. Conversely, USNORTHCOM is a purely US military organization based on the US UCP. USNORTHCOM forces operating in the same area as NORAD forces may provide tactical intercept information to NORAD forces. Conversely, NORAD air defense control assets may provide tactical intercept information to USNORTHCOM forces while they remain under the OPCON of their respective commander. To create combined effects, USNORTHCOM accomplishes coordination with numerous commands and agencies. For instance:

(1) USNORTHCOM plans, organizes, and, as directed, executes HD operations within the USNORTHCOM AOR in concert with missions performed by NORAD. The mission and geographic overlaps between NORAD and USNORTHCOM require both commands to coordinate and synchronize their operations.

(2) USNORTHCOM coordinates with NORAD and CJOC for the ground and maritime defense of North America.

(3) USNORTHCOM coordinates air defense operations with NORAD.

(4) To facilitate coordination, a *Memorandum of Understanding Between North American Aerospace Defense Command and United States Northern Command and Canadian Joint Operations Command Concerning the Exchange of Information Between the Three Commands of Commander's Critical Information Requirements and Other Information Requirements,* was codified on 25 January 2012.

b. **USSTRATCOM.** USSTRATCOM support to NORAD includes:

(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 accomplishment of both commands' missions.

c. **USTRANSCOM.** USTRANSCOM provides common-user and commercial air, land, and sea transportation; terminal management; patient movement; 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 main and forward operating bases are capable of supporting designated refueling and associated support operations.

(2) Support NORAD deployment, resupply, and redeployment with air, sea, and other assets, as directed by SecDef.

(3) Coordinate force movement requirements and related materials (including strategic aeromedical evacuation) involving common user lift.

d. **USPACOM.** USPACOM plans, organizes, and, as directed, executes HD operations within the USPACOM AOR. The mission and geographic proximity between NORAD and USPACOM require both commands to coordinate and synchronize their operations.

e. **USEUCOM.** USEUCOM's AOR extends across the Atlantic Ocean to the west coast of Greenland and west to approximately 45 degrees west longitude. NORAD's OA and USEUCOM's AOR overlap.

f. **USSOUTHCOM.** NORAD's OA and USSOUTHCOM's AOR overlap. NORAD has a memorandum of understanding with USSOUTHCOM to address issues of mutual concern, list support rendered by one party to the other, and deconflict their operations when necessary. Of particular interest to NORAD, this memorandum of understanding addresses CD operations and US military operations in the vicinity of Cuba.

g. **NORAD, CJOC, and USNORTHCOM.** NORAD supports CJOC and USNORTHCOM in their assigned missions to defend Canada and the US. NORAD is supported by both commands in the conduct of missions assigned to NORAD. NORAD provides bi-national aerospace and maritime situational awareness to CJOC and USNORTHCOM.

6. North American Aerospace Defense Command Subordinate Commands

a. NORAD aerospace warning and air control operations are conducted by its three subordinate regions. Each region has an air operations center and is further subdivided into one or more ADSs for tactical execution. The ADS operates a battle control center (BCC), a tactical C2 node that supports air battle management, air weapons control, surveillance and identification, data links, and airspace management.

b. Each BCC contains a combat mission crew and battle staff. When formed, the battle staff directs sector air control activities. The BCC operates on a continuous basis and closely coordinates air sovereignty activities with FAA air traffic control centers to ensure HD activities can be safely and successfully executed.

c. NORAD tactical-level operations also include ground-based air defense units in fixed locations (e.g., the NCR) and temporary sites, as needed, to support national special security events. Units supporting temporary sites (e.g., USAF control and reporting centers

and airborne warning and control systems) share air picture information with the associated BCC. A more detailed description of each of the three NORAD regions is provided below.

(1) **ANR.** ANR is the bi-national organization responsible for performing the NORAD air sovereignty and air control mission over the state of Alaska and the northwest approaches to North America. HQ ANR is collocated at Joint Base Elmendorf-Richardson, Alaska, with HQ US ALCOM, a subordinate unified command of USNORTHCOM. The ANR Commander is also the Commander, 11th Air Force, as well as commander of ALCOM. ANR is supported by both active duty Canadian forces and US forces, as well as Alaska ANG units. The ANR's BCC 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 Joint Base Elmendorf-Richardson.

(2) **Canadian North American Aerospace Defense Command Region (CANR).** CANR is the bi-national organization responsible for performing NORAD's air sovereignty and air control mission over Canada and the polar approaches to North America. CANR is located at Canadian Forces Base (CFB) Winnipeg, Manitoba. The BCC for Canada is located at CFB North Bay, Ontario. The CANR commander is also the commander of 1 CAD. CANR is manned by both 1 CAD and US personnel.

(3) **CONR.** CONR is the subordinate, bi-nationally staffed command responsible for the air sovereignty and air control of the airspace over the CONUS and the approaches to North America. The CONR commander exercises OPCON over all air defense forces within CONUS. CONR operates in a complex, bi-national, and multi-command environment where political, military, and economic conditions interrelate. CONR is collocated with 1st Air Force, a numbered air force subordinate to Air Combat Command. The CONR commander is also the CDRAFNORTH and may be designated the JFACC for USNORTHCOM for unilateral US air operations within the USNORTHCOM AOR. CONR ADSs and the NCR-IADS are identified below.

(a) **NCR-IADS.** NCR-IADS consists of two tactical C2 entities that provide air defense for the NCR under the OPCON of the CONR commander. The Eastern Air Defense Sector (EADS) is responsible for surveillance, identification, and air intercept operations, while the JADOC provides ground-based air defense forces to complement EADS capabilities. EADS and JADOC coordinate on all air tracks of interest within the NCR.

(b) **EADS.** EADS, located at Rome ANG Base, New York, is responsible for all CONR air operations east of the western boundary of the following states: Wisconsin, Illinois, Kentucky, Tennessee, and Alabama.

(c) **Western Air Defense Sector (WADS).** WADS, located at Joint Base Lewis-McChord, Washington, is responsible for all CONR air operations west of the eastern boundary of the following states: Minnesota, Iowa, Missouri, Arkansas, and Mississippi.

7. Other Forces

a. **USELEMNORAD.** USELEMNORAD is an organizational construct created in response to the requirements of Title 10, USC, which 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 bi-national command. CDRUSELEMNORAD is the senior US officer assigned to NORAD.

b. **1 CAD.** Winnipeg, Manitoba, is home to the dual HQ for 1 CAD and the CANR. The HQ serves 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 NORAD.

APPENDIX D
JOINT TASK FORCE HEADQUARTERS ENABLING CAPABILITIES POINTS OF CONTACT

Joint Staff/J7/Doctrine Division

Web Site:	http://www.jcs.mil/doctrine/
Email Support:	js.pentagon.j7.jedd-support@mail.mil
Phone number:	1-703-692-7273 (DSN 222)

Joint Staff Doctrine Sponsor/J35

At the time of this publication:

	JOD Americas
Comm:	1-703-697-9400
NIPR:	js.pentagon.j3.list.j35-ddro-jod-americas@mail.mil
SIPR:	js.pentagon.j3.list.j35-ddro-jod-americas@mail.smil.mil

Joint Enabling Capabilities Command (JECC)

Mailing Address:	9712 Virginia Ave. Building X-132
	Naval Station Norfolk, VA 23511
Web Site:	http://www.jecc.mil/

JECC Communication/Public Affairs:

	Phone: 757-836-8935
	DSN: 836-8935
	Email: transcom.jeccnews@mail.mil

24/7 JECC Watch Officer:

	Phone: 757-836-8939
	DSN: 836-8939
	Email: transcom.jeccewatchofficer@mail.mil

Defense Threat Reduction Agency (DTRA)

Mailing Address:	8725 John J. Kingman Rd. Stop 6201
	Ft. Belvoir, VA 22060-6201
Web Site:	http://www.dtra.mil/Home/Contact.aspx
Email:	dtra.publicaffairs@dtra.mil
Phone Number:	1-703-767-5870
Toll Free:	1-800-701-5096

Joint Personnel Recovery Agency (JPRA)

Mailing Address:	10244 Burbeck Road, Building 358
	Fort Belvoir, VA 22060-5805
Web Site:	https://public.jpra.mil/default.aspx

JPRA Operations Support Center

Phone Number:	(703) 704-4111

Defense Intelligence Agency (DIA)

Mailing Address: Office of Corporate Communications
Joint Base Anacostia Bolling
Building 6000
Washington DC 20340-5100
Web Site: http://www.dia.mil/
Phone Number: 202-231-5554
Email: DIA-PAO@dia.mil

Joint Warfighting Analysis Center (JWAC)

Mailing Address: Joint Warfare Analysis Center
4048 Higley Rd. Dahlgren, VA 22448-5144
Web Site: http://www.jwac.mil/
Phone Number: (540) 653-3749
(540) 653-3750

Defense Logistics Agency (DLA)

Mailing Address: DEFENSE LOGISTICS AGENCY
Andrew T. McNamara Building
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6221
Web Site: http://www.dla.mil/
INFORMATION/STAFF DUTY OFFICER (SDO)
SECURITY: 703-767-4010
SDO: 1600-0730/Weekends/Holidays: 703-767-5200

Joint Electronic Warfare Center (JEWC)

Mailing Address: U.S. Strategic Command
Public Affairs Office (J020)
901 SAC BLVD STE 1A1
Offutt Air Force Base, NE 68113 – 6020
Web Site: http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/978985/joint-electronic-warfare-center-jewc/
Phone Number: (402) 294-4130 (DSN 271)

APPENDIX E
REFERENCES

The development of JP 3-27 is based on the following primary references:

1. General

a. *United States Constitution*.

b. *Canada-United States Rush-Bagot Treaty*.

c. *Air Defense of the United States and Canada.*

d. Title 10, USC, *Armed Forces*.

e. Title 14, USC, *United States Coast Guard*.

f. Title 18, USC, Section 1385, *The Posse Comitatus Act*.

g. Title 32, USC, *National Guard*.

h. Title 33, USC, *Navigation and Navigable Waters*.

i. Title 46, USC, *Shipping*.

j. Title 50, USC, *War and National Defense*.

k. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act* (as amended).

2. Strategic Guidance and Policy

a. *National Strategy for Homeland Security*.

b. *National Strategy for Maritime Security*.

c. *National Strategy for Physical Protection of Critical Infrastructure and Key Assets*.

d. *National Strategy to Secure Cyberspace*.

e. *National Intelligence Strategy of the United States of America*.

f. *National Military Strategy of the United States of America*.

g. *The National Security Strategy of the United States of America*.

h. *National Response Framework*.

i. *National Strategy for Combating Terrorism*.

j. *Defense Strategic Guidance*.

k. *Maritime Strategy for Homeland Security*.

l. *Strategy to Combat Transnational Organized Crime*.

m. *National Defense Strategy of the United States of America*.

n. *National Geospatial-Intelligence Agency Geospatial Intelligence Series (GIPS)*.

o. *National Military Strategy for Cyberspace Operations*.

p. *Strategy for Homeland Defense and Defense Support of Civilian Authorities*.

q. *Unified Command Plan*.

r. *The Department of Defense Cyber Strategy*.

s. *DOD Strategy for Countering Weapons of Mass Destruction*.

t. HSPD-1, *Organization and Operation of the Homeland Security Council.*

u. HSPD-2, *Combating Terrorism Through Immigration Policies.*

v. HSPD-6, *Integration and Use of Screening Information.*

w. HSPD-10/NSPD-33, *Bio-defense for the 21st Century.*

x. HSPD-11, *Comprehensive Terrorist-Related Screening Procedures.*

y. HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors.*

z. HSPD-14/NSPD-43, *Domestic Nuclear Detection Office.*

aa. HSPD-15/NSPD-46, *US Policy and Strategy in the War on Terror.*

bb. HSPD-16/NSPD-47, *US Aviation Security Policy.*

cc. HSPD-18, *Medical Countermeasures Against Weapons of Mass Destruction.*

dd. HSPD-19, *Combating Terrorist Use of Explosives in the United States*.

ee. HSPD-23/NSPD 54, *U. S. Cyber Security Policy.*

ff. HSPD-59/NSPD-24, *Biometrics for Identification and Screening to Enhance National Security.*

gg. National Security Presidential Memorandum-4, *Organization of the National Security Council, the Homeland Security Council, and Subcommittees,* April 4, 2017.

hh. PPD-8, *National Preparedness.*

ii. PPD-10, *US Ballistic Missile Defenses.*

jj. PPD-17, *Countering Improvised Explosive Devices.*

kk. PPD-18, *Maritime Security.*

ll. PPD-21, *Critical Infrastructure Security and Resilience.*

mm. PDD-24, *US Counterintelligence.*

nn. PPD-25, *Guideline for U.S. Government Interagency Response to Terrorist Threats or Incidents in the U.S. and Overseas.*

oo. PPD-40, *National Continuity Policy.*

pp. PPD-42, (U) *Preventing and Countering Weapons of Mass Destruction Proliferation, Terrorism, and Use.*

qq. Presidential Decision Directive (PDD)-14, *Counternarcotics.*

rr. PDD-67, *Enduring Constitutional Government and Continuity of Government Operations.*

ss. EO 12333, *United States Intelligence Activities.*

tt. EO 12656, *Assignment of Emergency Preparedness Responsibilities.*

uu. EO 13223, *Ordering the Ready Reserve of the Armed Forces to Active Duty and Delegating Certain Authorities to the Secretary of Defense and the Secretary of Transportation.*

vv. EO 13228, *Establishing the Office of Homeland Security and the Homeland Security Council.*

ww. EO 13231, *Critical Infrastructure Protection in the Information Age.*

xx. EO 13381, *Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information.*

yy. EO 13385, *Continuance of Certain Federal Advisory Committees and Amendments to and Revocation of Other Executive Orders.*

zz. EO 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans.*

aaa. EO 13470, *Further Amendments to Executive Order 12333, United States Intelligence Activities*.

3. Department of Defense Publications

a. DODD 3020.26, *Department of Defense Continuity Programs.*

b. DODD 3020.40, *Mission Assurance (MA).*

c. DODD 3160.01, *Homeland Defense Activities Conducted by the National Guard.*

d. DODD 5100.01, *Functions of the Department of Defense and Its Major Components.*

e. DODD 5105.19, *Defense Information Systems Agency (DISA).*

f. DODD 5105.21, *Defense Intelligence Agency (DIA).*

g. DODD 5105.22, *Defense Logistics Agency (DLA).*

h. DODD 5105.62, *Defense Threat Reduction Agency (DTRA).*

i. DODD 5105.77, *National Guard Bureau (NGB).*

j. DODD 5105.83, *National Guard Joint Force Headquarters-State (NG JFHQs-State).*

k. DODD 5148.11, *Assistant to the Secretary of Defense for Intelligence Oversight (ATSD[IO]).*

l. DODD 5148.13, *Intelligence Oversight.*

m. DODD 5200.27, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense.*

n. DODD 5205.02E, *DOD Operations Security (OPSEC) Program.*

o. DODD 5210.56, *Arming and Use of Force.*

p. DODD 5240.01, *DOD Intelligence Activities.*

q. DODD 8000.01, *Management of Department of Defense Information Enterprise (DOD IE).*

r. DODD 8521.01E, *DOD Biometrics.*

s. DODI 2000.12, *DOD Antiterrorism (AT) Program.*

t. DODI O-2000.16, Volume 1, *DOD Antiterrorism (AT) Program Implementation: DOD AT Standards.*

u. DODI 3000.05, *Stability Operations.*

v. DODI 3001.02, *Personnel Accountability in Conjunction With Natural or Manmade Disasters.*

w. DODI 3020.41, *Operational Contract Support (OCS).*

x. DODI 3020.45, *Defense Critical Infrastructure Program (DCIP) Management.*

y. DODI 3020.52, *DOD Installation Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRNE) Preparedness Standards.*

z. DODI 3025.21, *Defense Support of Civilian Law Enforcement Agencies.*

aa. DODI 3115.12, *Open Source Intelligence*.

bb. DODI 5220.22, *National Industrial Security Program (NISP).*

cc. DODI 6055.17, *DOD Emergency Management (EM) Program.*

dd. DODI 8500.01, *Cybersecurity.*

ee. DODM 3020.45, Volume I, *Defense Critical Infrastructure Program (DCIP): DOD Mission-Based Critical Asset Identification Process (CAIP).*

ff. DODM 5240.01, *Procedures Governing the Conduct of DOD Intelligence Activities*

gg. DOD 5240.1-R *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons.*

hh. Global Force Management Guidance. Section II, *Assignment of Forces (Forces For Unified Commands).*

ii. *Joint Planning Guidance*.

jj. *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*.

kk. *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*.

ll. *Memorandum of Agreement Between the Department of Defense and the Department of Homeland Security on the Use of the United States Coast Guard Capabilities and Resources in Support of the National Maritime Strategy*.

mm. *The North American Aerospace Defense Command (NORAD) Agreement and Terms of Reference*.

nn. *Operation NOBLE EAGLE (ONE) Tactics, Techniques, and Procedures Reference Guide*.

oo. *Ballistic Missile Defense Review Report*.

pp. *Maritime Operational Threat Response (MOTR)*.

qq. *Contingency Planning Guidance*.

rr. *Canada-United States Basic Defense Document*.

ss. *Military Order of 13 November 2001*.

tt. *National Industrial Security Program*.

uu. Unified Facilities Criteria 4-010-01, *DOD Minimum Standards for Buildings.*

4. Chairman of the Joint Chiefs of Staff Publications

a. CJCSI 1301.01F, *Joint Individual Augmentation Procedures.*

b. CJCSI 3100.01C, *Joint Strategic Planning System.*

c. CJCSI 3121.01B, *(U) Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces.*

d. CJCSI 3213.01D, *Joint Operations Security.*

e. CJCSI 3610.01D, *Aircraft Piracy (Hijacking) and Destruction of Derelict Airborne Objects.*

f. CJCSI 3710.01B, *DOD Counterdrug Support.*

g. CJCSI 4120.02D, *List of Priorities—DOD Transportation Movement Priority System.*

h. CJCSI 5221.01D, *Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations.*

i. CJCSI 5810.01D, *Implementation of the DOD Law of War Program.*

j. CJCSM 3130.03, *Adaptive Planning and Execution (APEX) Formats and Guidance.*

k. JP 1, *Doctrine for the Armed Forces of the United States.*

l. JP 1-0, *Joint Personnel Support.*

m. JP 2-0, *Joint Intelligence.*

n. JP 2-01, *Joint and National Intelligence Support to Military Operations.*

o. JP 3-0, *Joint Operations.*

p. JP 3-01, *Countering Air and Missile Threats.*

q. JP 3-03, *Joint Interdiction.*

r. JP 3-07.2, *Antiterrorism.*

s. JP 3-07.4, *Counterdrug Operations.*

t. JP 3-08, *Interorganizational Cooperation.*

u. JP 3-09.3, *Close Air Support.*

v. JP 3-11, *Operations in Chemical, Biological, Radiological and Nuclear Environments.*

w. JP 3-12, *Cyberspace Operations.*

x. JP 3-13.2, *Military Information Support Operations.*

y. JP 3-13.3, *Operations Security.*

zz. JP 3-14, *Space Operations.*

aa. JP 3-15, *Barriers, Obstacles, and Mine Warfare for Joint Operations.*

bb. JP 3-16, *Multinational Operations.*

cc. JP 3-28, *Defense Support of Civil Authorities.*

dd. JP 3-30, *Command and Control of Joint Air Operations.*

ee. JP 3-31, *Command and Control for Joint Land Operations.*

ff. JP 3-32, *Command and Control for Joint Maritime Operations.*

gg. JP 3-33, *Joint Task Force Headquarters.*

hh. JP 3-34, *Joint Engineer Operations.*

ii. JP 3-35, *Deployment and Redeployment Operations.*

jj. JP 3-40, *Countering Weapons of Mass Destruction.*

kk. JP 3-41, *Chemical, Biological, Radiological, and Nuclear Response.*

ll. JP 3-52, *Joint Airspace Control.*

mm. JP 3-57, *Civil Military Operations*

nn. JP 3-60, *Joint Targeting.*

oo. JP 3-61, *Public Affairs.*

pp. JP 4-0, *Joint Logistics.*

qq. JP 4-02, *Joint Health Services.*

rr. JP 4-05, *Joint Mobilization Planning.*

ss. JP 4-06, *Mortuary Affairs.*

tt. JP4-10, *Operational Contract Support.*

uu. JP 5-0, *Joint Planning.*

vv. JP 6-0, *Joint Communications System.*

ww. *JG 1-05, Religious Affairs in Joint Operations.*

xx. JDN 3-16, *Joint Electromagnetic Spectrum Operations*.

5. Multi-Service Publications

a. ATP 3-22.40 (FM 3-22.40)/MCTP 10-10A (MCWP 3-15.8)/NTTP 3-07.3.2/AFTTP 3-2.45/CGTTP 3-92.2, *Multi-Service Tactics, Techniques, and Procedures for the Employment of Nonlethal Weapons.*

b. ATP 3-28.1/MCWP 3-36.2/NTTP 3-57.2/AFTTP 3-2.67, *Multi-Service Tactics, Techniques, and Procedures for Defense Support of Civil Authorities (DSCA).*

c. NTTP 3-07.11M/CGTTP 3-93.3/MCIP 3-33.04, *Visit, Board, Search, and Seizure Operations.*

6. Army Publications

a. Army Doctrine Publication (ADP) 1, *The Army.*

b. ADP 3-0, *Operations.*

7. Marine Corps Publication

Marine Corps Doctrinal Publication 1, *Warfighting.*

8. Navy Publications

a. Naval Doctrine Publication 1, *Naval Warfare.*

b. NWP 3-10, *Navy Expeditionary Combat Command Forces.*

c. NWP 3-32, *Maritime Operations at the Operational Level of War*.

d. NTTP 3-32.1, *Maritime Operations Center.*

9. Air Force Publications

a. Air Force Doctrine Volume 1, *Basic Doctrine.*

b. Air Force Doctrine Volume 3, *Command.*

c. Air Force Doctrine Annex 3-27, *Homeland Operations.*

d. Air Force Doctrine Annex 4-02, *Medical Operations.*

e. Air Force Instruction 10-2701, *Organization and Function of the Civil Air Patrol.*

10. Coast Guard Publications

a. COMDTINST M16247.1, *Maritime Law Enforcement Manual (MLEM).*

b. COMDTINST M16600.6, *Maritime Security and Response Operations (MSRO).*

c. COMDTINST M16000.3, *Underwater Port Security Operations Manual*.

d. COMDTINST M16000.11, *Marine Safety Manual, Volume VI, Ports and Waterways Activities*.

e. COMDTINST M16000.12, *Port Security Compliance Manual*.

f. COMDTINST M16790.1, *Auxiliary Manual*.

g. Coast Guard Publication 1, *Doctrine for the US Coast Guard*.

h. Coast Guard Publication 3-0, *Operations*.

i. Coast Guard Publication 3-2, *Short Notice Maritime Response*.

11. National Guard Publications

a. CNGB Instruction, 2000.01, *National Guard Intelligence Activities*.

b. CNGB Manual, 2000.01, *National Guard Intelligence Activities*.

APPENDIX F
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication using the Joint Doctrine Feedback Form located at: https://jdeis.js.mil/jdeis/jel/jp_feedback_form.pdf and e-mail it to: js.pentagon.j7.mbx.jedd-support@mail.mil. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

a. The lead agent for this publication is US Northern Command. The Joint Staff doctrine sponsor for this publication is the Director for Operations (J-3).

b. The following staff, in conjunction with the joint doctrine development community, made a valuable contribution to the revision of this joint publication: lead agent, Mr. Mark Clements, US Northern Command; Joint Staff doctrine sponsor, LCDR Justin Cooper, Joint Staff J-3; Mr. Robert Brodel, Joint Staff J-7, Joint Doctrine Analysis Division; and Lt Col Mark Newell, Joint Staff J-7, Joint Doctrine Division.

3. Supersession

This publication supersedes JP 3-27, *Homeland Defense,* 29 July 2013.

4. Change Recommendations

a. To provide recommendations for urgent and/or routine changes to this publication, please complete the Joint Doctrine Feedback Form located at: https://jdeis.js.mil/jdeis/jel/jp_feedback_form.pdf and e-mail it to: js.pentagon.j7.mbx.jedd-support@mail.mil.

b. When a Joint Staff directorate submits a proposal to the CJCS 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 Services and other organizations are requested to notify the Joint Staff J-7 when changes to source documents reflected in this publication are initiated.

5. Lessons Learned

The Joint Lessons Learned Program (JLLP) primary objective is to enhance joint force readiness and effectiveness by contributing to improvements in doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy. The Joint Lessons Learned Information System (JLLIS) is the DOD system of record for lessons learned and facilitates the collection, tracking, management, sharing, collaborative resolution, and dissemination of lessons learned to improve the development and readiness of the joint force. The JLLP integrates with joint doctrine through the joint doctrine development process by

providing lessons and lessons learned derived from operations, events, and exercises. As these inputs are incorporated into joint doctrine, they become institutionalized for future use, a major goal of the JLLP. Lessons and lessons learned are routinely sought and incorporated into draft JPs throughout formal staffing of the development process. The JLLIS Website can be found at https://www.jllis.mil (NIPRNET) or http://www.jllis.smil.mil (SIPRNET).

6. Distribution of Publications

Local reproduction is authorized, and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified JPs must be IAW DOD Manual 5200.01, Volume 1, *DOD Information Security Program: Overview, Classification, and Declassification,* and DOD Manual 5200.01, Volume 3, *DOD Information Security Program: Protection of Classified Information.*

7. Distribution of Electronic Publications

a. Joint Staff J-7 will not print copies of JPs for distribution. Electronic versions are available on JDEIS Joint Electronic Library Plus (JEL+) at https://jdeis.js.mil/jdeis/index.jsp (NIPRNET) and http://jdeis.js.smil.mil/jdeis/index.jsp (SIPRNET), and on the JEL at http://www.jcs.mil/Doctrine/ (NIPRNET).

b. Only approved JPs are releasable outside the combatant commands, Services, and Joint Staff. Defense attachés may request classified JPs by sending written requests to Defense Intelligence Agency (DIA)/IE-3, 200 MacDill Blvd., Joint Base Anacostia-Bolling, Washington, DC 20340-5100.

c. JEL CD-ROM. Upon request of a joint doctrine development community member, the Joint Staff J-7 will produce and deliver one CD-ROM with current JPs. This JEL CD-ROM will be updated not less than semi-annually and when received can be locally reproduced for use within the combatant commands, Services, and combat support agencies.

GLOSSARY
PART I—ABBREVIATIONS, ACRONYMS, AND INITIALISMS

AC	Active Component
ADP	Army doctrine publication
ADS	air defense sector
AFTTP	Air Force tactics, techniques, and procedures
ALCOM	United States Alaskan Command
ANG	Air National Guard
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
ASD(HD&GS)	Assistant Secretary of Defense (Homeland Defense and Global Security)
AT	antiterrorism
ATO	air tasking order
ATP	Army techniques publication
BCC	battle control center
BMD	ballistic missile defense
BSI	base support installation
C2	command and control
CAA	command arrangement agreement
CAD	Canadian air division
CAIS	civil authority information support
CANR	Canadian North American Aerospace Defense Command Region
CAP	Civil Air Patrol
CBRN	chemical, biological, radiological, and nuclear
CCDR	combatant commander
CCMD	combatant command
CD	counterdrug
CDC	Centers for Disease Control and Prevention (DHHS)
CDRAFNORTH	Commander, Air Force North
CDRNORAD	Commander, North American Aerospace Defense Command
CDRUSAFRICOM	Commander, United States Africa Command
CDRUSARNORTH	Commander, United States Army, North
CDRUSCENTCOM	Commander, United States Central Command
CDRUSELEMNORAD	Commander, United States Element, North American Aerospace Defense Command
CDRUSEUCOM	Commander, United States European 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	Chief of Defence Staff (Canada)
CFB	Canadian forces base
CG	commanding general
CGDEFOR	Coast Guard defense force
CGTTP	Coast Guard tactics, techniques, and procedures
CI	counterintelligence
CI/KR	critical infrastructure and key resources
CIP	critical infrastructure protection
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSM	Chairman of the Joint Chiefs of Staff manual
CJOC	Canadian Joint Operations Command
CJTF	commander, joint task force
CM	cruise missile
CMOC	civil-military operations center
CNGB	Chief, National Guard Bureau
CO	cyberspace operations
COCOM	combatant command (command authority)
COG	continuity of government
COMDTINST	Commandant instruction (USCG)
COMPACAF	Commander, Pacific Air Forces
COMUSNAVNORTH	Commander, United States Naval Forces, Northern Command
COMUSPACFLT	Commander, United States Pacific Fleet
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
CS&C	Office of Cybersecurity and Communications (DHS)
CSA	combat support agency
CSS	combat service support
CT	counterterrorism
CWMD	countering weapons of mass destruction
DC3	Department of Defense Cyber Crime Center
DCE	defense coordinating element
DCI	defense critical infrastructure

DCIP	Defense Critical Infrastructure Program
DCISE	Defense Industrial Base Collaborative Information Sharing Environment
DCMA	Defense Contract Management Agency
DCO	defensive cyberspace operations
DFBA	Defense Forensics and Biometrics Agency
DHHS	Department of Health and Human Services
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIB	defense industrial base
DIRLAUTH	direct liaison authorized
DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DODIN	Department of Defense information network
DODM	Department of Defense manual
DOE	Department of Energy
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
DSCA	defense support of civil authorities
DTRA	Defense Threat Reduction Agency
EADS	Eastern Air Defense Sector
EMIO	expanded maritime interception operations
EO	executive order
EP	emergency preparedness
EPLO	emergency preparedness liaison officer
EXORD	execute order
FAA	Federal Aviation Administration (DOT)
FBI	Federal Bureau of Investigation (DOJ)
FEMA	Federal Emergency Management Agency (DHS)
FHP	force health protection
FM	field manual (Army)
FP	force protection
GCC	geographic combatant commander
GEF	Guidance for Employment of the Force
GEOINT	geospatial intelligence
GMD	ground-based midcourse defense
HD	homeland defense
HQ	headquarters

HS	homeland security
HSC	Homeland Security Council
HSPD	homeland security Presidential directive
IAA	incident awareness and assessment
IAMD	integrated air and missile defense
IAW	in accordance with
IC	intelligence community
ICBM	intercontinental ballistic missile
IO	information operations
ITW/AA	integrated tactical warning and attack assessment
J-1	manpower and personnel directorate of a joint staff
JADOC	Joint Air Defense Operations Center (NORAD)
JCS	Joint Chiefs of Staff
JDN	joint doctrine note
JFACC	joint force air component commander
JFC	joint force commander
JFCC Space	Joint Functional Component Command for Space (USSTRATCOM)
JFHQ-NCR	Joint Force Headquarters-National Capital Region
JFLCC	joint force land component commander
JFMCC	joint force maritime component commander
JG	joint guide
JIATF-S	Joint Interagency Task Force-South
JIATF-W	Joint Interagency Task Force-West
JIDO	Joint Improvised-Threat Defeat Organization (DTRA)
JIOC	joint intelligence operations center
JOA	joint operations area
JP	joint publication
JRSOI	joint reception, staging, onward movement, and integration
JTF	joint task force
JTF-HD	Joint Task Force-Homeland Defense
JTF-N	Joint Task Force-North
JTTF	joint terrorism task force
LE	law enforcement
LEA	law enforcement agency
LFA	lead federal agency
LNO	liaison officer
MA	mortuary affairs
MARFORNORTH	United States Marine Corps Forces North
MCIP	Marine Corps interim publication
MCM	mine countermeasures

MCTP	Marine Corps tactical publication
MCWP	Marine Corps warfighting publication
MDA	Missile Defense Agency
MDIOC	Missile Defense Integration and Operations Center (MDA)
MHD	maritime homeland defense
MHS	maritime homeland security
MIO	maritime interception operations
MISO	military information support operations
MOTR	maritime operational threat response
NATO	North Atlantic Treaty Organization
NCIJTF-AG	National Cyber Investigative Joint Task Force-Analytical Group (DOD)
NCR	National Capital Region (US)
NCRCC	National Capital Region Coordination Center
NCR-IADS	National Capital Region-Integrated Air Defense System
NCTC	National Counterterrorism Center
NDDOC	North American Aerospace Defense Command and United States Northern Command Deployment and Distribution Operations Cell
NEST	nuclear emergency support team (DOE)
NG	National Guard
NGA	National Geospatial-Intelligence Agency
NGB	National Guard Bureau
NG JFHQ-State	National Guard joint force headquarters-state
NGO	nongovernmental organization
NIMS	National Incident Management System
NMS	national military strategy
NORAD	North American Aerospace Defense Command
NRF	National Response Framework
NSA	National Security Agency
NSC	National Security Council
NSPD	national security Presidential directive
NSS	national security strategy
NST	National Geospatial-Intelligence Agency support team
NTTP	Navy tactics, techniques, and procedures
NWP	Navy warfare publication
OA	operational area
OCO	offensive cyberspace operations
OCS	operational contract support
OE	operational environment
ONE	Operation NOBLE EAGLE
OPCON	operational control
OPLAN	operation plan

PA	public affairs
PCA	Posse Comitatus Act
PDD	Presidential decision directive
PN	partner nation
PPD	Presidential policy directive
PWCS	port, waterways, and coastal security
QRF	quick response force
RC	Reserve Component
RFF	request for forces
ROE	rules of engagement
RRF	rapid response force
RS	religious support
RST	religious support team
RUF	rules for the use of force
SATCOM	satellite communications
SCA	space coordinating authority
SecDef	Secretary of Defense
SIGINT	signals intelligence
SIOC	Strategic Information and Operations Center (FBI)
SOCNORTH	United States Special Operations Command, North
SOCPAC	Special Operations Command Pacific
SOF	special operations forces
SPP	State Partnership Program
SROE	standing rules of engagement
SRUF	standing rules for the use of force
TAA	tactical assembly area
TACON	tactical control
TAG	the adjutant general
TCO	transnational criminal organization
TCP	theater campaign plan
TMM	transregional, multi-domain, and multifunctional
TSA	Transportation Security Administration (DHS)
TSOC	theater special operations command
UA	unmanned aircraft
UAS	unmanned aircraft system
UCP	Unified Command Plan
USA	United States Army
USAF	United States Air Force
USARNORTH	United States Army, North
USARPAC	United States Army, Pacific Command
USC	United States Code

USCG	United States Coast Guard
USCYBERCOM	United States Cyber Command
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
USMC	United States Marine Corps
USN	United States Navy
USNORTHCOM	United States Northern Command
USPACOM	United States Pacific 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
WRA	weapons release authority

PART II—TERMS AND DEFINITIONS

aerospace defense. Defensive measures designed to destroy or nullify attacking enemy aircraft and missiles and also negate hostile space systems. (Approved for incorporation into the DOD Dictionary.)

air sovereignty. A nation's inherent right to exercise absolute control and authority over the airspace above its territory. (DOD Dictionary. Source: JP 3-27)

critical infrastructure and key resources. The infrastructure and assets vital to a nation's security, governance, public health and safety, economy, and public confidence. Also called **CI/KR.** (DOD Dictionary. Source: JP 3-27)

defense critical infrastructure. Department of Defense and non-Department of Defense networked assets and facilities essential to project, support, and sustain military forces and operations worldwide. Also called **DCI.** (DOD Dictionary. Source: JP 3-27)

defense industrial base. The Department of Defense, government, and private sector worldwide industrial complex with capabilities to perform research and development and design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements. Also called **DIB.** (Approved for incorporation into the DOD Dictionary.)

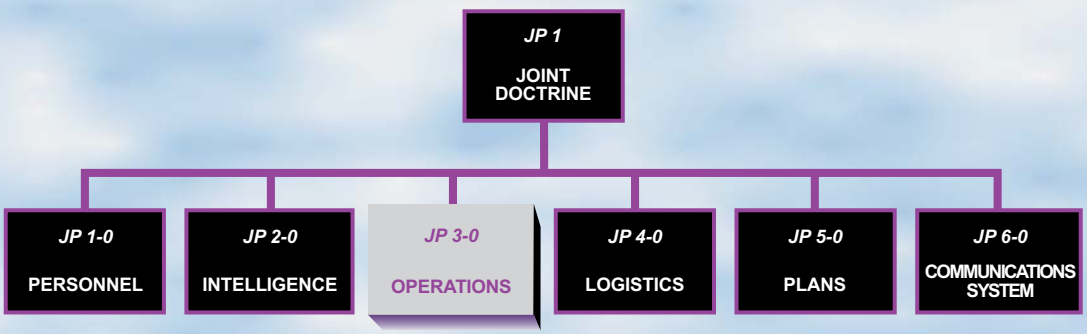
domestic emergencies. Civil defense emergencies, civil disturbances, major disasters, or natural disasters affecting the public welfare and occurring within the United States and its territories. (DOD Dictionary. Source: JP 3-27)

homeland defense. The protection of United States sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression or other threats as directed by the President. Also called **HD.** (DOD Dictionary. Source: JP 3-27)

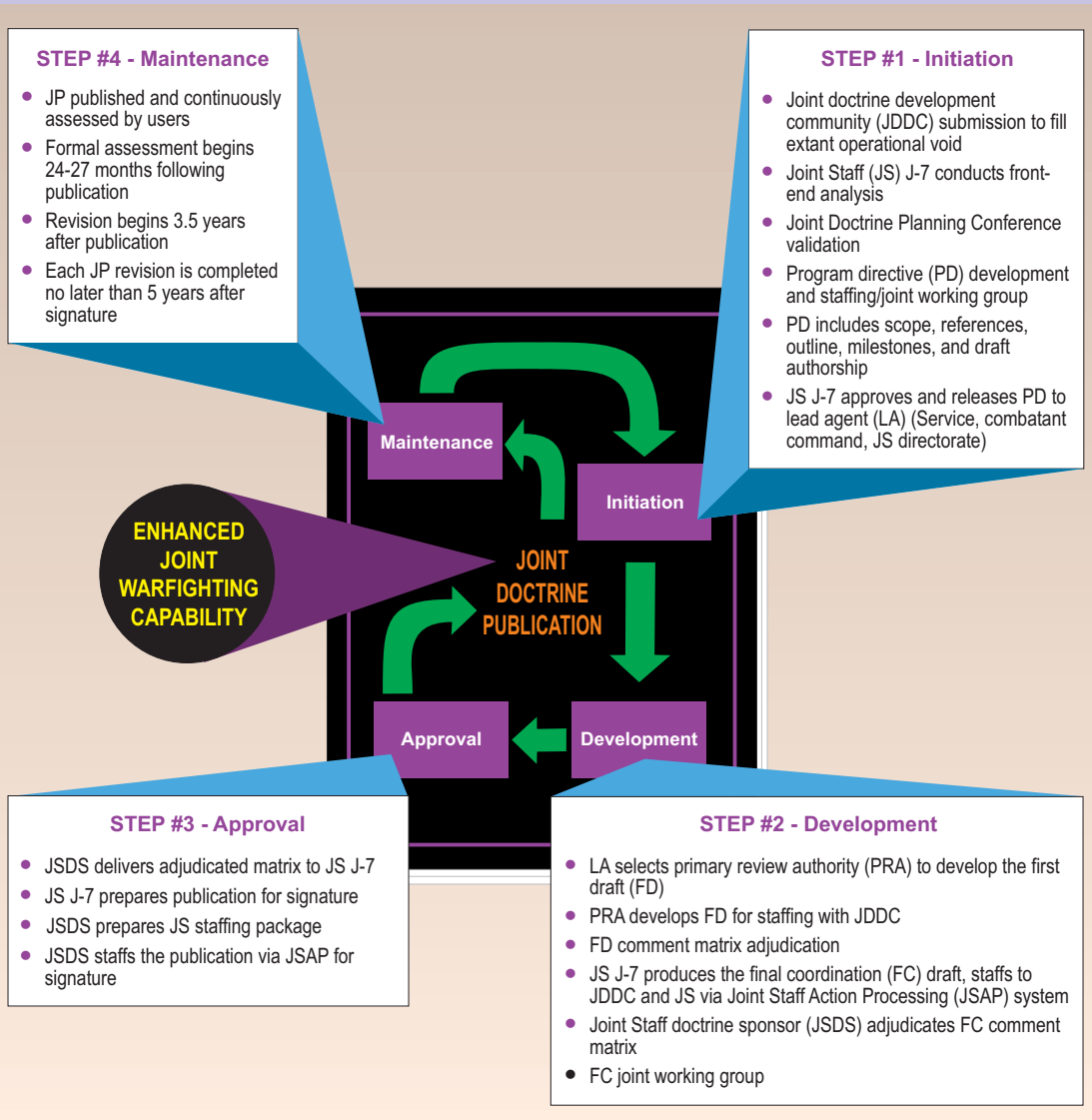
homeland security. A concerted national effort to prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism, major disasters, and other emergencies; and minimize the damage and recover from attacks, major disasters, and other emergencies that occur. Also called **HS.** (DOD Dictionary. Source: JP 3-27)

national preparedness. Actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the nation. (Approved for inclusion in the DOD Dictionary.)

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