

# Joint Publication 3-26



# Homeland Security



2 August 2005



# PREFACE

## 1. Scope

This publication provides joint doctrine to guide the Armed Forces in the conduct of homeland security operations. It describes the homeland security framework, mission areas, missions and related supporting operations and enabling activities. It also discusses legal authorities; joint force, multinational, and interagency relationships; command and control; planning and execution; and training and resource considerations.

## 2. Purpose

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

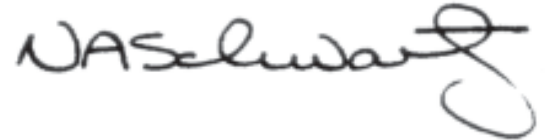
## 3. Application

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

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

c. Defense support of civil authorities is a new term and is approved in the National Response Plan and is not yet approved in Department of Defense (DOD) policy. Once it is approved in DOD policy, it will likely replace civil support as the overarching term for assistance to civil authorities. However, in the context of this publication, civil support is still used as the overarching term.

For the Chairman of the Joint Chiefs of Staff:

A handwritten signature in black ink, appearing to read "NASchwartz", with a large, stylized flourish at the end.

NORTON A. SCHWARTZ  
Lieutenant General, USAF  
Director, Joint Staff

# TABLE OF CONTENTS

	PAGE
EXECUTIVE SUMMARY .....	v
CHAPTER I	
INTRODUCTION	
• General .....	I-1
• Threats .....	I-4
• Department of Defense Approach to Homeland Security .....	I-8
• Department of Defense Contribution to Homeland Security .....	I-10
• Department of Defense Homeland Security Framework .....	I-10
• Legal and Policy Considerations .....	I-14
CHAPTER II	
COMMAND RELATIONSHIPS AND INTERAGENCY RESPONSIBILITIES	
• General .....	II-1
• Command and Control Relationships and Responsibilities .....	II-3
• Federal Agency Responsibilities and Considerations .....	II-14
• Non-Department of Defense Federal Agencies and Responsibilities .....	II-17
• Special Considerations .....	II-21
CHAPTER III	
HOMELAND DEFENSE	
• General .....	III-1
• Homeland Defense Operational Elements and Characteristics .....	III-2
• Homeland Defense Missions .....	III-4
• Supporting Operations and Enabling Activities .....	III-5
• Planning Considerations for Homeland Defense Operations .....	III-9
CHAPTER IV	
CIVIL SUPPORT	
• General .....	IV-1
• Civil Support Characteristics .....	IV-2
• Civil Support Mission Area .....	IV-4
• Supporting Operations and Enabling Activities .....	IV-7
• Department of Defense Civil Support Process .....	IV-10
• Planning Considerations for Civil Support Operations .....	IV-13

APPENDIX

A	Key Homeland Security Legal and Policy Documents .....	A-1
B	Combat Support Agencies and Capabilities .....	B-1
C	References .....	C-1
D	Administrative Instructions .....	D-1

GLOSSARY

Part I	Abbreviations and Acronyms .....	GL-1
Part II	Terms and Definitions .....	GL-5

FIGURE

I-1	National Strategy for Homeland Security .....	I-2
I-2	Department of Defense’s Operational Descriptions of Homeland Security and Mission Areas .....	I-3
I-3	Relationship of Emergency Preparedness to Homeland Security Mission Areas .....	I-4
I-4	Homeland Security Strategic Threat Environment .....	I-6
I-5	Critical Infrastructure Protection Framework .....	I-8
I-6	Homeland Defense and Civil Support Operational Framework .....	I-12
I-7	Notional Homeland Security Campaign Model .....	I-14
I-8	Sources of Guidance for the Homeland Security Mission .....	I-15
II-1	Geographic Combatant Commanders Areas of Responsibility .....	II-2
II-2	Organization Chart: Office of the Assistant Secretary of Defense for Homeland Defense .....	II-6
II-3	Guidelines for Interagency Coordination .....	II-16
II-4	Lead Federal Agency/Department of Defense Relationships .....	II-17
II-5	Department of Homeland Security .....	II-19
III-1	Homeland Defense Missions and Operational Elements .....	III-2
III-2	Homeland Defense Missions .....	III-5
IV-1	Civil Support Missions .....	IV-4
IV-2	Military Support to Civil Authorities .....	IV-5
IV-3	Military Assistance for Civil Disturbance Operations .....	IV-8
IV-4	Relationship Between Crisis Management and Consequence Management .....	IV-9
IV-5	Examples of Critical Infrastructure .....	IV-10
IV-6	Request for Assistance .....	IV-11
B-1	Combat Support Agencies .....	B-1

## EXECUTIVE SUMMARY COMMANDER'S OVERVIEW

- **Discusses the Department of Defense (DOD) Contribution to Homeland Security and DOD Homeland Security Operational Framework**
  - **Covers Command and Control Relationships Within DOD and Interagency Relationships**
  - **Discusses DOD Homeland Defense Missions, to Include Supporting Operations and Enabling Activities**
  - **Covers DOD Civil Support Missions, to Include Supporting Operations and Enabling Activities**
- 

### The Strategic Context

*The homeland, described as the physical region that includes the continental United States, Alaska, Hawaii, US territories and possessions, and surrounding territorial waters and airspace, is exposed to the possibility of harm from hostile states or non-state actors at all times.*

*The Armed Forces of the United States conduct planning and operations to prepare to detect, deter, prevent and defeat threats and aggression aimed at the US, its territories, and interests, and to mitigate the impact of adversary actions.*

To preserve the freedoms guaranteed by the Constitution of the United States, **the Nation must have a homeland that is secure from threats and violence, including terrorism.** Homeland security (HS) is the Nation's first priority, and it requires a national effort. The Department of Defense (DOD) has a key role in that effort. The National Strategy for Homeland Security (NSHS) complements the National Security Strategy of the United States by providing a comprehensive framework for organizing the efforts of federal, state, local, and private organizations whose primary functions are often unrelated to national security. Critical to understanding the overall relationship is an understanding of the distinction between the role that DOD plays with respect to securing the Nation and HS, and the policy in the NSHS, which has the Department of Homeland Security (DHS) as the lead. **HS at the national level has a specific focus on terrorist threats. The DOD focus in supporting HS is broader.**

Military application of the NSHS calls for preparation, detection, deterrence, prevention, defending, and responding to threats and aggression aimed at the homeland. The DOD also provides military assistance to civil authorities (MACA), including consequence management (CM) activities. **The Armed Forces of the United States support the NSHS through two distinct but interrelated mission areas — homeland defense (HD) and civil support (CS).**

**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.**

DOD is responsible for homeland defense, which includes missions such as domestic air defense. DOD recognizes that threats planned or inspired by "external" actors may materialize internally. The reference to "external threats" does not limit where or how attacks could be planned and executed. DOD is prepared to conduct homeland defense missions whenever the President, exercising his constitutional authority as Commander in Chief, authorizes military actions. For HD missions, as directed by the President of the United States and/or the Secretary of Defense (SecDef), DOD is the lead or primary agency .

**DOD's role in the CS mission area consists of support to US civil authorities** for domestic emergencies, and for designated law enforcement within the scope of restrictions required by the Posse Comitatus Act and other support approved by the SecDef. The SecDef provides military assistance to US civil authorities for domestic incidents as directed by the President and consistent with military readiness, Department of Defense directives, and the law.

### Department of Defense Homeland Security Framework

*The Department of Defense (DOD) framework is characterized by preparation, detection, deterrence, preemption, defense, and respond.*

DOD "prepares and responds" when conducting both HD and CS. DOD primarily focuses on "detect, deter, preempt, and defend" when they conduct HD missions.

**Prepare.** Emergency preparedness is a shared responsibility and a partnership that includes the Federal government, state and local agencies, the private sector, and individual citizens.

**Detect.** Early detection of threats is essential. Detection is a national effort, which involves maintaining a common operational picture and the sharing and fusing of information/intelligence through a network of federal, state, and local agencies.

**Deter.** An effective deterrence requires the adversary leadership to believe the United States has both the ability and will to preempt or retaliate promptly with responses that are credible and effective.

**Preempt.** Preemption consists of proactive measures taken to prevent or neutralize a perceived or imminent attack. Preemption may include offensive actions such as air strikes, maritime interception, or direct action.

**Defend.** HD missions are those that protect the Nation’s sovereignty.

**Respond.** Response, as it relates to HS activities, spans both HD and CS mission areas.

### Command Relationships

*The President and Secretary of Defense or their designated representatives exercise authority and control of the Armed Forces of the United States through the chain of command described in Joint Publication 0-2, Unified Action Armed Forces (UNAAF), and DOD policy.*

**Regardless of whether DOD is conducting HD or CS, military forces will always remain under the control of the established Title 10, 32, or state active duty military chain of command.**

**For HD missions, DOD is in the lead with other federal agencies in support.** DOD’s capability to respond quickly to any threat or situation places a high demand on the same resources. For example, the same force trained and ready to execute its mission that has been constituted to achieve objectives outside the homeland may also be required to execute HD missions within the homeland.

**In certain circumstances, military commanders or responsible officials in other DOD components may be faced with situations that will require them to provide immediate response to civil authorities.** Responses to requests from civil authorities prior to receiving authority from the President or chain of command are made when immediate support is critical to save lives, prevent human suffering, or to mitigate great property damage. Such requests are situation specific, time-sensitive, and may or may not be associated with a declared disaster. When such conditions exist and time does not permit prior approval from higher headquarters, commanders or officials acting under immediate response authority may take necessary action to respond, but must advise the National Military Command Center through command channels by the most expeditious means available and seek approval or additional authorizations.

*Commander, US Northern Command*

**Commander, United States Northern Command (CDRUSNORTHCOM)** has specific responsibilities for HD and for supporting civil authorities. United States Northern Command's (USNORTHCOM's) mission is to conduct operations to deter, prevent, and defeat threats and aggression aimed at the United States, its territories, and interests within the assigned area of responsibility (AOR) and as directed by the President or SecDef, provide military assistance to civil authorities including CM operations. USNORTHCOM embodies the principles of unity of effort and unity of command as the single, responsible, designated DOD commander



for overall command and control of DOD support to civil authorities within the USNORTHCOM AOR. CDRUSNORTHCOM takes all operational orders from and is responsible to the President through SecDef.

### Federal Agency Responsibilities and Considerations

*DOD is one of many federal agencies and organizations with homeland security responsibilities.*

There are interagency groups and plans in which DOD is an active participant. Except for HD missions, DOD will serve in a supporting role for domestic incident management. **Working in concert forges the vital links between the military instrument of national power and the economic, diplomatic and informational instruments of the US Government.** Synchronization and integration of all instruments of national power is required to ensure the successful execution of HS missions. The challenges facing the Nation are increasingly complex and will require the skills and resources of many organizations. Guidelines for interagency coordination include: achieve unity of effort among a mix of federal, state and local agencies; identify all agencies and organizations potentially involved in the operation; identify key elements of information that various agencies can share; establish an interagency hierarchy for the response effort; identify appropriate resources of each participant; define the objectives of the response effort; define the desired end state and exit criteria; define courses of action for the supporting effort; identify potential obstacles; maximize the mission's assets to support long-term goals; and establish interagency assessment teams.

### Homeland Defense

*Under the DOD homeland defense mission area military capabilities are used to counter threats and aggression against the United States.*

**DOD is the lead, supported by other agencies, in defending against traditional external threats/aggression (e.g., air and missile attack).** However, against internal asymmetric, non-traditional threats (e.g., terrorism), DOD may be in support of DHS. **When ordered to conduct HD operations within US territory, DOD will coordinate closely with other federal agencies or departments.** Consistent with laws and policy, the Services will provide capabilities to support combatant command requirements against a variety of air, land, maritime, space, and cyber incursions that can threaten national security. These include invasion, computer network attack, and air and missile attacks. The purpose of HD is to protect against and mitigate the impact of incursions or attacks on sovereign territory, the domestic population, and defense critical infrastructure.

## Civil Support

*DOD shall cooperate with and provide support to civil authorities as directed by and consistent with laws, Presidential directives, Executive Orders, and DOD policies and directives.*

**Employment of military forces within the US, its territories, and possessions, under the auspices of CS, typically falls under the broad mission of MACA.** MACA missions consist of three mission subsets. These mission subsets consist of: military support to civil authorities (MSCA); military support to civilian law enforcement agencies; and military assistance for civil disturbances.

**Military Support to Civil Authorities.** MSCA refers to support provided by Federal military forces, DOD civilians, contractor personnel, and DOD agencies and components in response to requests for assistance during domestic incidents to include terrorist threats or attacks, major disasters, and other emergencies. MSCA missions consist of DOD support to US domestic emergencies and for designated law enforcement, civil disturbances, and other activities.

**Military Support to Civilian Law Enforcement Agencies.** The use of the military in law enforcement roles is a sensitive topic and restrictions apply to such use. Military forces performing in this role support the lead Federal agency and other supporting agencies and may be armed depending on the SecDef decision. Military support to civilian law enforcement agencies (LEAs) may include, but is not limited to national special security events, support for combating terrorism, support to counterdrug operations, maritime security, intelligence, surveillance, and reconnaissance capabilities, and general support (training support to LEAs/loan of equipment/personnel and expert advice).

**Military Assistance for Civil Disturbances.** The President is authorized by the Constitution and statutory laws to employ the Armed Forces of the United States to suppress insurrections, rebellions, and riots, and provide federal supplemental assistance to the states to maintain law and order. Responsibility for the management of federal response for civil disturbances rests with the Attorney General.

## Conclusion

This publication provides joint doctrine to guide the Armed Forces in the conduct of homeland security operations. It describes the homeland security framework, mission areas, missions and related supporting operations and enabling activities. It also discusses legal authorities; joint force, multinational, and interagency relationships; command and control; planning and execution; and training and resource considerations.

Intentionally Blank

## CHAPTER I INTRODUCTION

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

**President George W. Bush**

### 1. General

The homeland, described as the physical region that includes the continental United States (CONUS), Alaska, Hawaii, US territories and possessions, and surrounding territorial waters and airspace, is exposed to the possibility of harm from hostile states or non-state actors at all times. The Nation must always be vigilant against such dangers. To preserve the freedoms guaranteed by the Constitution of the United States, the Nation must have a homeland that is secure from threats and violence, including terrorism. **Homeland security (HS) is the Nation’s first priority, and it requires a national effort. The Department of Defense (DOD) has a key role in that effort.** The National Strategy for Homeland Security (NSHS) complements the National Security Strategy (NSS) of the United States by providing a comprehensive framework for organizing the efforts of federal, state, local, and private organizations whose primary functions are often unrelated to national security. **Critical to understanding the overall relationship is**



*To preserve the freedoms guaranteed by the Constitution of the United States, the Nation must have a homeland that is secure from threats and violence, including terrorism.*

**an understanding of the distinction between the role that DOD plays with respect to securing the Nation and HS, and the policy in the NSHS, which has the Department of Homeland Security (DHS) as the lead.** HS at the national level has a specific focus on terrorist threats. The DOD focus in supporting HS is broader.

a. As part of an integrated national strategy, military power is applied in concert with the other instruments of national power — diplomatic, informational, and economic. The diversity of threats and challenges requires that the military instrument of national power take a broad role in preparing, detecting, deterring, preempting, defending, and responding to threats or acts of terrorism. Our national military objective to defend the homeland takes into account our national interests to ensure US security and freedom of action. Ultimately, the execution of our strategy is focused on the security of the United States. Adversary perceptions of US military capabilities and intent are fundamental to creating a deterrent effect. The effectiveness of deterrence, power projection, and other strategic concepts hinges on the US ability to influence the perceptions and behavior of others.

b. The NSHS identifies the following strategic objectives: **reducing our Nation’s vulnerabilities to terrorism, preventing terrorist attacks, minimizing the damage, and recovering from attacks that do occur.** In order to enhance the security of the homeland, the following critical areas will require increased emphasis: indications and warning; border and transportation security; domestic counterterrorism; national critical infrastructure and key assets (NCI&KA) protection; international cooperation; interoperability; and emergency preparedness (EP) and response (Figure I-1).



Figure I-1. National Strategy for Homeland Security

(1) To support the NSHS, the Armed Forces of the United States, in accordance with guidance established in the National Military Strategy (NMS), conduct planning and operations to prepare, detect, deter, prevent, and defeat threats and aggression aimed at the US, its territories, and interests, and to mitigate the impact of adversary actions.

(2) Military application of the NSHS calls for preparation, detection, deterrence, prevention, defending, and responding to threats and aggression aimed at the homeland. DOD also provides military assistance to civil authorities (MACA), including consequence management (CM) activities. **The Armed Forces of the United States support the NSHS through two distinct but interrelated mission areas — homeland defense (HD) and civil support (CS).** Figure I-2 is a broad operational description of HS that includes both NSHS and DOD contributions. The descriptions of HD and CS in the figure represent the DOD’s role in carrying out the NSHS. The mission area descriptions provide an overarching perspective and do not necessarily identify all of the specific actions performed by various agencies.



Figure I-2. Department of Defense's Operational Descriptions of Homeland Security and Mission Areas

(a) **HD is the protection of US territory, sovereignty, domestic population, and critical infrastructure against external threats and aggression.** For HD missions, as directed by the President of the United States and/or the Secretary of Defense (SecDef), DOD serves as the lead federal agency (LFA).

(b) **DOD’s role in the CS mission area consists of support to US civil authorities** for domestic emergencies, and for designated law enforcement within the scope of restrictions required by the Posse Comitatus Act (PCA) and other support approved by SecDef. SecDef provides MACA for domestic incidents as directed by the President and consistent with military readiness, Department of Defense directives (DODDs), and the law.

(3) **To ensure DOD’s readiness for the HD and CS mission areas, DOD must also engage in EP.** EP consists of those planning activities undertaken to ensure DOD processes, procedures, and resources are in place to support the President and SecDef, and as required, other federal departments and agencies in a designated national security emergency. EP is considered a part of DOD’s overall preparedness activities. **Within DOD, it is not considered a stand-alone activity, but an integral part of training and preparation.** Figure I-3 illustrates how HD, CS, and EP are connected and related to national HS efforts.

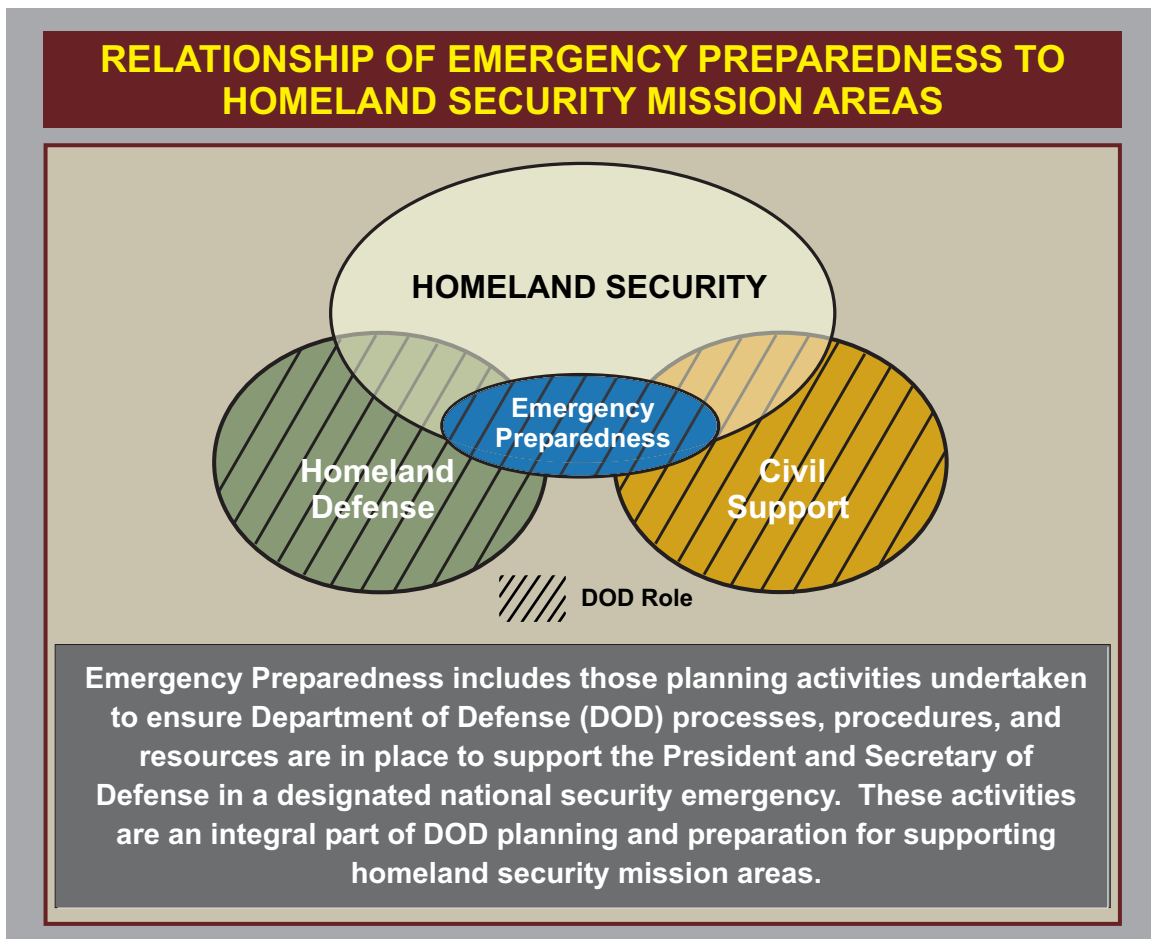


Figure I-3. Relationship of Emergency Preparedness to Homeland Security Mission Areas

(4) To orchestrate the myriad of capabilities associated with NSHS, DOD must closely coordinate efforts with DHS, and other Federal, state, and local government agencies, and the private sector, and facilitate information/intelligence sharing to ensure unity of effort. Since many HS objectives are best accomplished by building upon existing capabilities, the Federal government's role is to support and enhance those capabilities already at the state and local level. To do this, DHS coordinates federal activities, integrates national preparedness and response systems, and encourages development and enhancement of state and local capabilities.

## 2. Threats

In today's complex threat environment, **our approach to security must continue to address both external and internal aspects.** Externally, the US has sought to shape the international environment through the application of diplomatic, economic, military, informational, and cultural engagement. Internally, our culture, societal norms, and when required, our justice system provides for domestic peace and tranquility. Attacks from within and outside our borders have exposed vulnerabilities. Given the persistent nature of current threats, a proactive, comprehensive approach to HS is required. The uncertainty of the strategic environment is influenced by numerous factors (see Figure I-4).

a. An adversary's choice of weapons to threaten the US homeland range from conventional means of attack or delivery to chemical, biological, radiological, nuclear, or high-yield explosives (CBRNE) weapons. Attacks can also include non-kinetic weapons directed at information systems and other critical infrastructure. Weapons and tactics designed to kill or terrorize large numbers of people or destroy facilities of strategic importance are within the capabilities of many of our adversaries.

b. Evidence of threats can be clearly observed by noting adversary efforts to develop and field long-range ballistic missiles and the proliferation of technologies to develop weapons of mass destruction (WMD) and the means to deliver them. Terrorist attacks in New York City, Washington, DC, Pennsylvania, and Oklahoma City have highlighted adversary capabilities and asymmetric approaches. **Successfully countering traditional and asymmetric threats and reducing risk will require a concerted and coordinated effort by DOD and other federal agencies as well as by state and local governments and each citizen.** Similar coordination will be required to mitigate the consequences of attacks.

c. A complex, uncertain, and volatile threat environment has emerged that presents the US with a resource-intensive challenge at home and abroad in the event of a future conflict. Our world is smaller today because of the ease with which information can be made available. Adversaries have taken advantage of this technology and employ it in their own operations, in areas such as moving money, communicating with cells in their organizations, approving missions, or conducting surveillance and reconnaissance on potential targets. A number of regional powers, non-state actors, and transnational groups possess the capability to challenge the interests of the US and those of our allies. All are expected to continue improving their capabilities. **The number of adversaries that may threaten our ability to protect our interests is increasing at a rapid pace.** In spite of intensive counterproliferation and arms control efforts, the likelihood that adversaries will employ WMD against





Figure I-4. Homeland Security Strategic Threat Environment

the US or its interests has increased. A CBRNE attack could come in a variety of forms, from release through conventional means such as a ballistic missile to unconventional means like a “suitcase” radiological device.

d. **America remains vulnerable to large-scale terrorist attacks.** Evidence suggests that terrorist organizations have grown more extreme in their objectives and actions and are less concerned that attacks on innocent civilians or public infrastructure will undermine support for their causes. Some groups have attained a considerable degree of financial independence and essentially “declared war” on the US with little regard as to how we will respond.

*See Joint Publication (JP) 3-07.2, Joint Tactics, Techniques, and Procedures for Antiterrorism, for more information on countering terrorist threats.*

e. **America’s critical infrastructure includes a number of interrelated sectors.** Our agricultural, utilities, industrial and services sectors of the economy are interdependent, and along with the public health and emergency services sectors, provide the goods and services essential to the Nation. Our institutions of government guarantee our national security and freedom, and administer key public functions. Our defense industrial base provides essential resources for military capabilities to help safeguard our population from external threats and support force projection and sustainment. Our information and telecommunications sectors enable economic productivity and growth, and are particularly important because they connect and help control many other critical infrastructure assets. Our energy, transportation, banking and finance, chemical industry, agricultural, and postal and shipping sectors help sustain our economy and touch the lives of the Nation daily. Because many of the assets associated with the critical infrastructure of the US are interrelated or part of an integrated system, a successful attack on one critical node could have a devastating impact on others and the country overall.



*America remains vulnerable to large-scale terrorist attacks.*

f. Today, only a few countries possess the capability to conduct a conventional military strike on our homeland, but the emergence of hostile non-state actors, the proliferation of WMD, and new forms of asymmetric conflict combine to make defending the homeland more complex. Protection of defense critical infrastructure (DCI) (e.g., power projection platforms, ports, airfields, and command and control systems) and support to other agencies in protecting or mitigating the consequences of attacks on NCI&KA remains essential tasks for the Armed Forces of the United States (see Figure I-5).

g. **There is a persistent threat to our national borders posed by the influx of illegal immigrants, drugs and contraband.** This poses a serious threat to the Nation and requires the combined efforts of law enforcement agencies (LEAs), intelligence agencies, and when requested and approved, support from DOD assets to enhance LEA efforts to secure our borders and conduct counter illicit trafficking operations. However, only in unique and/or extraordinary circumstances would DOD take the lead to secure our borders.

*See JP 3-07.4, Joint Doctrine for Counterdrug Operations.*

h. **Significant events of high public interest present lucrative targets for adversaries intent on disrupting our national sense of security.** Presidential decision directive (PDD) 62, *Combating Terrorism*, formalized the roles and responsibilities of federal agencies in the development of security plans for major events. When an event is designated by the Secretary of the Department of Homeland Security per Homeland Security Presidential Directive (HSPD)-7 a national special security event (NSSE), the United States Secret Service (USSS), as part of DHS, assumes the role of lead agency for the design and implementation of the operational security plan.



Figure I-5. Critical Infrastructure Protection Framework

### 3. Department of Defense Approach to Homeland Security

**DOD contributes to HS through HD and CS. DOD support to HS is global in nature and is often conducted in depth beginning at the source of the threat. Applying military power at the source of the threat furthers the present strategy of deterrence.** This approach encompasses a range of deterrence strategies, including the prospect of certain overwhelming retaliation, preemption through a neutralizing first strike, and seamless defenses across all domains. In addition, the DOD approach to HS recognizes the critical importance of mitigating the consequences of an attack if deterrence and prevention should fail. An active, layered defense stretches across the integrated global battlespace. This battlespace consists of the forward regions, the approaches to the US, and the American homeland. In each of these areas, DOD must defend against attacks, whether launched by a hostile nation state or a transnational group.

a. **The Forward Regions**—the regions outside the homeland (land, air, sea, and space). In the forward regions, the objective is to detect, deter, or when directed, defeat threats to the homeland before they arise. Actions span the range of military operations and may include engagement activities, peace operations, or other preemptive measures such as direct action missions, computer network

attack and defense or global strikes on threats before they are employed. Some examples of operations conducted in the forward regions include surveillance and reconnaissance, active missile defenses, space operations, and air and maritime interdiction.

b. **The Approaches** — the region extending from the limits of the homeland to the forward region. The approaches are not uniformly defined, may not have boundaries and are normally based on situation-specific intelligence and the threat. Once intelligence has indicated that a threat is en route to the homeland from a foreign point of origin, it may be considered to be in the approaches. The primary objective of actions within the approaches is to locate and defeat threats as far from the homeland as possible.

c. **The Homeland** — the region that includes CONUS, Alaska, and Hawaii; US territories and possessions; and the surrounding territorial waters and airspace. In this region, the DOD objective is to defend against and defeat the threat. Defensive actions in the homeland normally take place simultaneously and in coordination with operations conducted in the approaches and/or forward regions. **Operations conducted in the homeland region include air, land, and maritime missions.** In addition, DOD may be required within this region to assist civil authorities in managing the consequences of attacks, incidents, and events that have already occurred.

d. It is important to note that the divisions among **all three regions are not absolute and they may overlap or shift depending on the situation and threat** therefore, all military operations associated with HS will require seamless integration and synchronization.



*All military operations associated with homeland security will require seamless integration and synchronization.*

#### 4. Department of Defense Contribution to Homeland Security

**DOD contributes to the NSHS through its missions overseas, HD, and CS.** However, it is imperative to understand that DOD’s role extends beyond the NSHS paradigm. Specific roles that are essential to DOD’s efforts to secure the homeland include:

- a. Ongoing missions abroad to reduce the threat of attacks against the US.
- b. Protecting the sovereignty, territory, domestic population, and critical defense infrastructure of the United States.
- c. Supporting civilian authorities for law enforcement, response to domestic emergencies, protection of NCI&KA, and other activities as directed.
- d. Ensuring that EP resources and procedures are in place in order to support other agencies that may require assistance.

#### 5. Department of Defense Homeland Security Framework

a. The organizational construct of the HS mission is best addressed within an overarching framework. **This framework is characterized by the following: prepare, detect, deter, preempt, defend, and respond.**

b. DOD “prepares and responds” when conducting both HD and CS. DOD primarily focuses on “detect, deter, preempt, and defend” when they conduct HD missions.

(1) **Prepare.** The nature of HS dictates that the Federal government alone cannot ensure the security of the homeland. EP is a shared responsibility and a partnership that includes the Federal government, state and local agencies, the private sector, and individual citizens. Each plays a crucial role and must be prepared to respond immediately to any threat.

(2) **Detect.** Early detection of threats is essential. Detection is a national effort, which involves maintaining a shared situational awareness through a common operational picture (COP) and the sharing and fusing of information/intelligence with a network of federal, state, and local agencies.

(3) **Deter.** An effective deterrence requires the adversary leadership to believe the United States has both the ability and will to preempt or retaliate promptly with responses that are credible and effective. Deterrence can be achieved by being so prepared for the attack that no advantage would be gained by an adversary. In addition, information/intelligence gathering and investigative efforts may also deter an attack.

(4) **Preempt.** Preemption consists of proactive measures taken to prevent or neutralize a perceived or imminent attack. Preemption may include offensive actions such as air strikes, maritime interception, or direct action. Intelligence gathering efforts, and possibly investigative efforts, are critical for the prosecution of successful preemptive actions. Preemption measures also exist to protect our homeland against illegal drug smuggling and immigration.



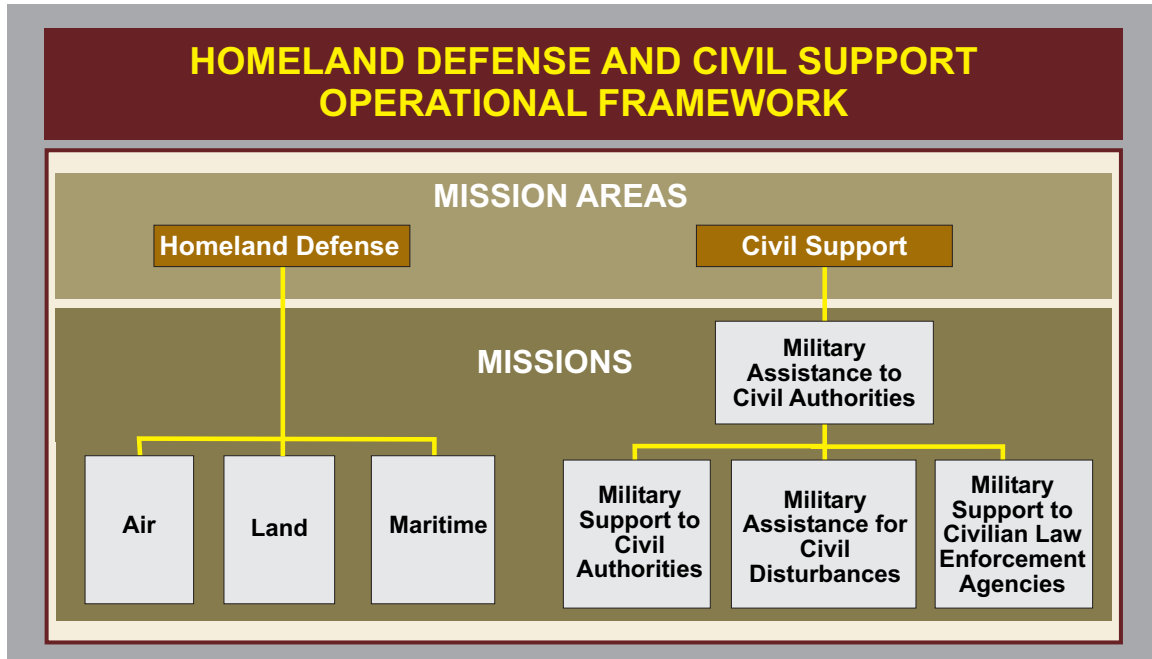
*Actions to defend the homeland contribute towards the goal of rendering hostile attacks ineffective.*

(5) **Defend.** HD missions are those that protect the Nation’s sovereignty. Active and passive defense measures that are mutually supporting and placed in effect before an anticipated attack are especially beneficial. Actions to defend the homeland contribute towards the goal of rendering hostile attacks ineffective.

(6) **Respond.** Response, as it relates to HS activities, spans both HD and CS mission areas. For HD, responding is the ability to rapidly deter, repel, or defeat an attack. DOD also provides discrete resources in the form of intelligence or operational capabilities. In the CS role, it is the ability to rapidly and effectively support civil authorities in managing the consequences of disasters and catastrophes, including natural, manmade, or terrorist incidents.

c. **DOD Homeland Defense and Civil Support Operational Framework.** The overarching operational framework for DOD support to HS consists of two mission areas — HD and CS. These mission areas contain a number of unique missions, mission subsets, supporting operations and enabling activities which can overlap. Synchronization and integration of selected HD and CS mission areas, supporting operations, actions, programs and enabling activities will be required. For example, force protection (FP) actions and the DOD antiterrorism (AT) program are applicable to both HD and CS missions. Mission areas and missions for DOD support to HS are depicted in Figure I-6.

d. **An integral part of the HD and CS mission areas is support to continuity of operations (COOP) and continuity of government (COG).** Federal, state and local government agencies have COOP plans for their vital functions. These plans will ensure continuation of minimum essential functions throughout the range of consequences from natural disasters to acts of terrorism. COOP planning



**Figure I-6. Homeland Defense and Civil Support Operational Framework**

normally includes: line of succession, delegation of authorities, alternate facilities and safekeeping of records, operating procedures, security, and communications. The COG program ensures the continued performance of essential functions and support of the President during national security emergencies. COG is basic to the survival of the Nation and ensures no power vacuum at any government level occurs that could lead to an unlawful assumption of authority. COG guidelines are contained in executive orders (EOs) and National Security Council (NSC) action documents.

*For further detail concerning COOP, refer to DODD 3020.26, Defense Continuity Program, and Chairman of the Joint Chiefs of Staff (CJCS) Operation Order 3-04.*

e. **Within HD there are air missions, land missions, and maritime missions.** Although these missions are described in the context of the defense, HD missions include offensive actions (preemptive activities to deter, disrupt and destroy adversary capabilities at their source). Supporting operations and enabling activities associated with HD missions may include: critical infrastructure protection (CIP) when directed, FP and AT, space operations, ballistic missile defense (BMD), and information operations (IO).

f. **Employment of military forces** within the US, its territories, and possessions provided under the auspices of CS, typically **falls under the broad mission of MACA. MACA operations consist of three subordinate missions.** They may overlap and DOD may, depending on the circumstances, provide support to them simultaneously. **They are military support to civil authorities (MSCA), military support to civil law enforcement agencies (MSCLEA), and military assistance for civil disturbances (MACDIS).** Military activities and operations associated with CS missions include, but are not limited to domestic CBRNE crisis management (CrM), and CM, counterdrug (CD) operations, maritime security, NSSE support activities, disaster responses, border security, AT activities, intelligence sharing, EP activities, and IO.



*Employment of military forces within the US typically falls under the broad mission of military assistance to civil authorities.*

g. Logistics is the foundation for maintaining a strong and ready military. From the strategic to the tactical level, **logistics is essential to the Nation’s ability to project combat power.** The NSHS recognizes that DOD is called upon regularly to provide assistance to civil authorities to deal with natural disasters (e.g., hurricanes, floods, and fires), as well as manmade incidents (e.g., riots and drug trafficking). The military is called on to perform these missions because it is able to move and organize large numbers of trained personnel to provide a coordinated response to incidents at home. The military has developed specialized capabilities (particularly, engineering and CBRNE weapons system response capabilities) that are critical to many types of CS operations. Each HS incident that requires United States Northern Command (USNORTHCOM) or United States Pacific Command (USPACOM) assistance to civil authorities will involve a different size and mix of forces. Specialized military capabilities are deployed based on SecDef approval of a request for support. Regardless of the mix of forces and equipment or the type of operation, logistic operations will be required. These operations will require early and integrated planning among the Services, sustaining organizations, combat support agencies, and other federal agencies as required.

h. **Essential to DOD participation in HS activities is the construct of campaign planning.** The example depicted in JP 3-0, *Doctrine for Joint Operations*, and the overarching procedures outlined in JP 5-0, *Doctrine for Planning Joint Operations*, are equally applicable to the HD and CS mission areas. Figure I-7 depicts a notional homeland security campaign planning model.





Figure I-7. Notional Homeland Security Campaign Model

## 6. Legal and Policy Considerations

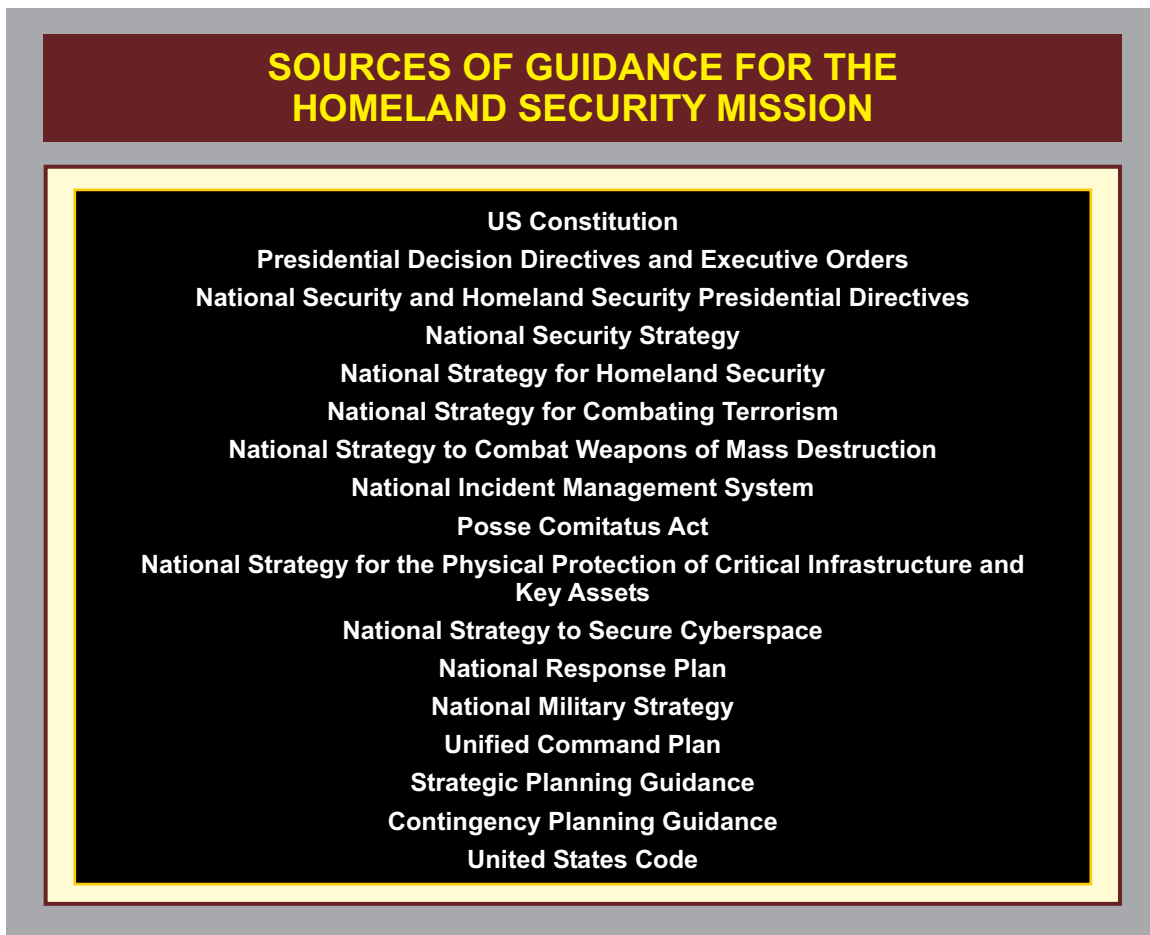
There are a variety of documents that provide guidance for supporting HS. These range from the US Constitution to the Contingency Planning Guidance (CPG). Figure I-8 lists a number of the key documents that will assist military forces in the performance of the HD and CS mission areas.

a. **Basic Principles.** The Constitution provides the fundamental justification for HS activities through the guarantee of domestic tranquility and the provision for the common defense of the Nation. To ensure those principles survive, the executive, legislative, and judicial branches of government issue and review key guidance using a variety of means, primarily through the President and Congress. These DODDs, policy documents, and laws provide the fundamental basis for the development of subordinate and implementing guidance by DOD agencies.

b. **Key Executive and Legislative Guidance.** PDDs, national security Presidential directives (NSPDs), HSPDs, and EOs are the primary means by which the President issues national security policy guidance. There have been a number of key documents issued by the national leadership impacting on the defense of the homeland. A list of documents that provide guidance for the HS mission is included in Appendix A, "Key Homeland Security Legal and Policy Documents."

### c. Key Department of Defense Guidance

(1) **Implications.** DOD guidelines are promulgated in a variety of documents that include national strategy documents, planning guidance, and DODDs. These policy documents are consistent



**Figure I-8. Sources of Guidance for the Homeland Security Mission**

with and complementary to the federal statutes and national security policy discussed earlier in this chapter. DODDs specifically address missions for HD and CS operations. A list of key DOD guidance is provided in Appendix A, “Key Homeland Security Legal and Policy Documents.”

(2) **Special Considerations.** Functional areas impacting HS are numerous. The following discussion provides general guidelines for intelligence operations and psychological operations (PSYOP), two areas that have specific applications when employed in an HS operation. They also have specific legal implications of which commanders should be aware.

(a) **Intelligence Operations.** The US military has a limited role in collecting foreign intelligence in domestic operations. Collection of counterintelligence is allowed and required to protect US Government property and human resources. Any information of possible foreign intelligence value that the Services may have obtained in a counterintelligence or domestic operation must be turned over to the Federal Bureau of Investigation (FBI), which has the primary responsibility for domestic intelligence collection within the United States. The Patriot Act eases some of the restrictions on foreign intelligence gathering within the United States, and affords the US intelligence community greater access to information gathered during criminal investigations. DOD intelligence activities are governed by the following references: EO 12333, *United States Intelligence Activities* (lays out the goals and direction of the national

intelligence effort, and describes the roles, responsibilities and restrictions of the different elements of the US intelligence community); Deputy Secretary of Defense Memorandum, “Collecting, Reporting and Analysis of Terrorist Threat to DOD Within the United States,” 2 May 2003; DODDs 5240.1, *DOD Intelligence Activities*, and 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons* (implement the guidance contained in EO 12333 as it applies to DOD); guidance for the collection of information on terrorists is contained in the 27 January 1998 Command, Control, Communications Intelligence Memorandum: “Authority to Collect Information on Domestic Terrorist and Other Groups Committing Illegal Acts that Pose a Threat to DOD.” SecDef Message dated 151147Z NOV 01, “Policy Guidance — Impact of USA PATRIOT Act of 2001 on DOD Intelligence Activities and Intelligence Oversight,” clarifies that the Act does not change the framework of DOD intelligence activities and does not change intelligence oversight guidance. DODD 5200.27, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense*, also pertains.

(b) **PSYOP.** US law prohibits PSYOP units from conducting operations against US citizens. However, these assets can be used to help disseminate critical information to the civilian population. PSYOP unit personnel and equipment may be used for such support activities as information dissemination, printing, reproduction, distribution, and broadcasting.

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

## CHAPTER II

### COMMAND RELATIONSHIPS AND INTERAGENCY RESPONSIBILITIES

*“In uniform, when I talk about terrorism it’s easy to assume that the war on terrorism is a military thing. It’s not at all. It demands the attention and action of all elements of national power.”*

**Gen. Richard B. Myers**  
Chairman of the Joint Chiefs of Staff

#### 1. General

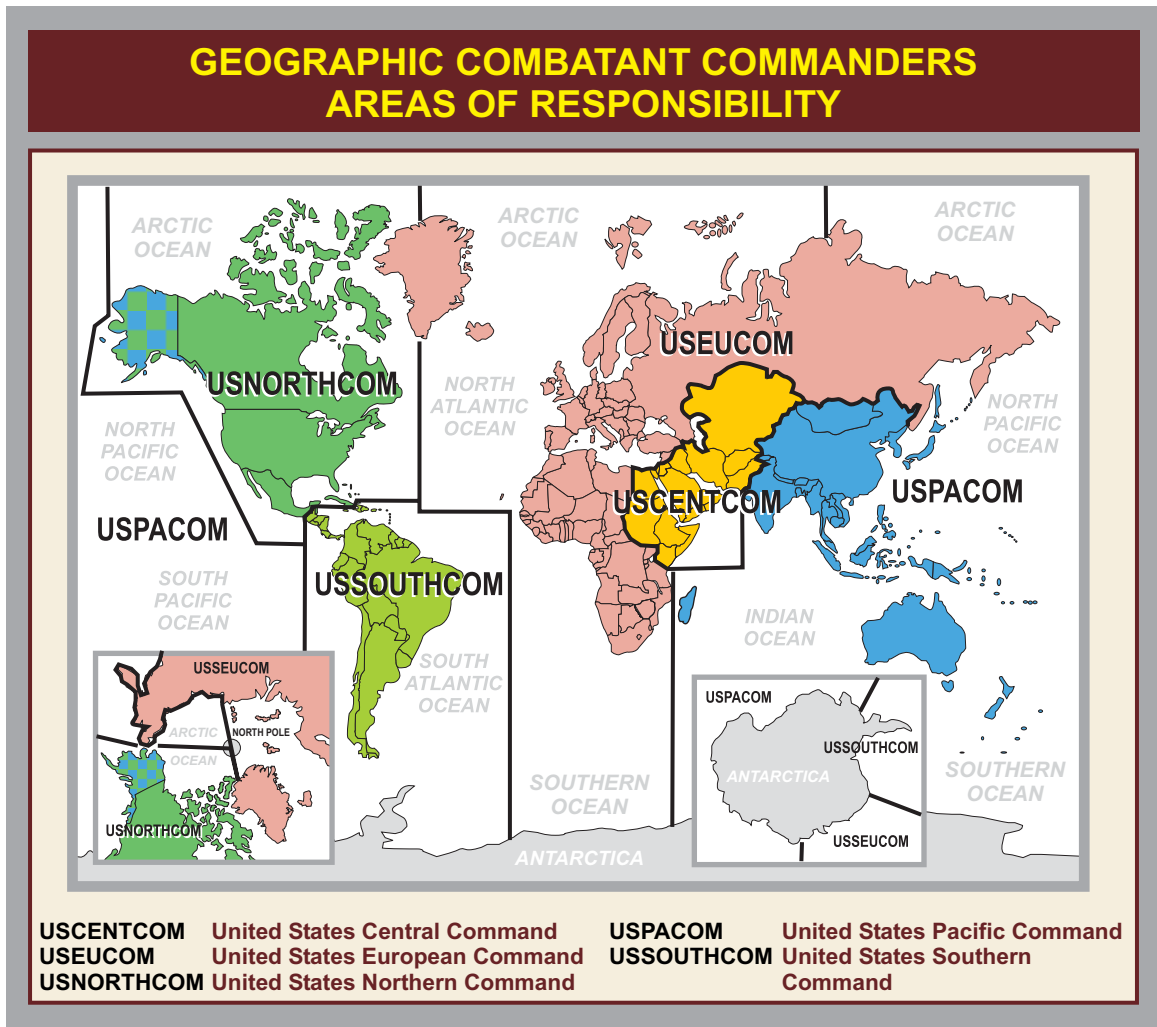
a. **The President exercises authority and control of the Armed Forces within DOD through two distinct branches of the chain of command.** One branch runs from the President, through SecDef, to commanders of combatant commands for missions and forces assigned to their commands. The other branch, used for purposes other than operational direction of forces assigned to the combatant commands, runs from the President through SecDef to Secretaries of the Military Departments. Military Departments, organized separately, operate under the authority, direction and control of SecDef. Secretaries of the Military Departments exercise authority through their respective Service Chiefs over their forces not assigned to the combatant commanders.

b. The combatant commanders exercise combatant command (command authority) (COCOM) of assigned forces, and are directly responsible to the President and SecDef for the performance of assigned missions and the preparedness of their commands. (Figure II-1 depicts the geographic combatant commands areas of responsibility [AORs].) Combatant commanders prescribe the chain of command within their commands and designate the appropriate authority to be exercised by subordinate commanders. Unless otherwise directed by the President or SecDef, COCOM is reserved for the commanders of the combatant commands and cannot be delegated or transferred. Subordinate commanders in the chain of command exercise authority (operational control [OPCON], tactical control [TACON], or a support command relationship) as prescribed by law or a superior commander.

*For detailed discussion of command relationships, see JP 0-2, Unified Action Armed Forces (UNAAF).*

c. The Military Departments operate under the authority, direction, and control of the SecDef. This branch of the chain of command embraces all military forces within the respective Service not assigned to commanders of combatant commands.

d. **HS related military operations inside the US and its territories**, though limited in many respects, **fall into two mission areas: HD**—for which **DOD serves as the LFA** and military forces are used to conduct military operations in defense of the homeland; and **CS**—**for which DOD normally serves in a supporting role to other agencies** by providing military assistance to civil authorities at the federal, state, and local levels. The President and SecDef define the circumstances under which DOD would be involved in the HD and CS missions.



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

(1) For HD missions, the President, exercising his constitutional authority as Commander in Chief, authorizes military action to counter threats to and within the United States. **Within the HD mission area, DOD conducts air missions, land missions, and maritime missions**, executes FP actions, DCI protection, BMD, and IO commensurate with mission requirements.

**(2) Civil Support**

(a) When operating within the CS mission area, DOD will be in support of another LFA. The domestic operating environment for military CS presents many challenges to the joint force commander. It is imperative that commanders and staffs at all levels understand the relationships, statutory and operational, among all federal agencies involved in the operation. Moreover, it is equally important to understand DOD's role in supporting these other federal agencies. **DOD will provide military assistance to the LFA and/or other primary agencies upon request by the appropriate authority and approval by SecDef. There are various national-level plans, such as the National Response Plan (NRP) and the National Incident Management System (NIMS), which detail the roles and missions of various federal**



*Within the civil support mission area, circumstances may arise that fall into the realm of emergency and temporary non-emergency incidents.*

**departments and agencies in the event of a domestic crisis.** The NRP provides detail for the roles and missions of various Federal departments and agencies in the event of a domestic crisis. The NIMS is part of the NRP and provides an operational framework to implement tenets of the NRP.

(b) Within the CS mission area, circumstances may arise that fall into the realm of emergency and temporary non-emergency incidents. **In emergency circumstances, such as managing the consequences of a terrorist attack, natural disaster, CIP, or other events, DOD could be asked to provide capabilities that other agencies do not possess or that have been exhausted or overwhelmed.**

## **2. Command and Control Relationships and Responsibilities**

a. The President and SecDef or their designated representatives exercise authority and control of the Armed Forces of the United States through the chain of command described in JP 0-2, *Unified Action Armed Forces (UNAAF)*, and DOD policy. **Regardless of whether DOD is conducting HD or CS, military forces will always remain under the control of the established Title 10, 32, or State Active Duty military chain of command.**

b. **For HD missions, DOD is in the lead with other federal agencies in support.** DOD's capability to respond quickly to any threat or situation places a high demand on the same resources. For example, the same trained and ready force constituted to achieve objectives outside the homeland may also be required to execute HD missions within the homeland. Guidelines for command and control (C2), as depicted in JP 0-2, *Unified Action Armed Forces (UNAAF)*, are equally applicable to HD operations.



*Under certain circumstances, military commanders are allowed to take necessary action under immediate response authority.*

c. **In certain circumstances, military commanders or responsible officials in other DOD components may be faced with situations that will require them to provide immediate response to civil authorities.** Responses to requests from civil authorities prior to receiving authority from SecDef are made when immediate support is critical to save lives, prevent human suffering, or to mitigate great property damage. Such requests are situation specific, time-sensitive, and may or may not be associated with a declared disaster. When such conditions exist and time does not permit prior approval from higher headquarters, commanders or officials acting under immediate response authority may take necessary action to respond, and shall report the request through the command channels to the National Military Command Center (NMCC) by the most expeditious means available. The military will begin disengagement from emergency response activity as soon as practicable.

*For more information on immediate response authority see DODD 3025.15, Military Assistance to Civil Authorities, and DODD 3025.1, Military Support to Civil Authorities.*

d. **Principal and supporting DOD participants involved in the execution of HD or CS mission areas** may include SecDef; Assistant Secretary of Defense for Homeland Defense [ASD(HD)]; Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict [ASD(SO/LIC)]; Assistant Secretary of Defense for Health Affairs [ASD(HA)]; Assistant Secretary of Defense for Reserve Affairs [ASD(RA)]; CJCS; Commander, North American Aerospace Defense Command (CDRNORAD); Commander, US Northern Command (CDRUSNORTHCOM); Commander, US Pacific Command (CDRUSPACOM); Commander, US Strategic Command (CDRUSSTRATCOM); Commander, US Special Operations Command (CDRUSSOCOM); Commander, US Transportation Command (CDRUSTRANSCOM); Commander, US Joint Forces Command (CDRUSJFCOM); Commander,

US Southern Command (CDRUSSOUTHCOM); and the Services. The Army and Air National Guard (ANG) are included when under Title 10 status. The US Coast Guard (USCG) is a participant from outside of DOD with authority to conduct Title 10 missions.

(1) **Secretary of Defense.** SecDef has overall authority for DOD and is the President's principal advisor on military matters concerning HS. Authority for the conduct and execution of the HD mission resides with SecDef. For civil support, SecDef retains approval authority for the use of forces, personnel, units, and equipment. SecDef has the primary responsibility within DOD to provide the overall policy and oversight for CS in the event of a domestic incident.

(2) **Assistant Secretary of Defense for Homeland Defense.** The Office of ASD(HD) is within the office of the Under Secretary of Defense for Policy [USD(P)]. ASD(HD) is responsible for the overall supervision of all DOD HD related activities. Within CS, ASD(HD) has been delegated the duties and authorities associated with principal staff assistant for MSCA and MACDIS. ASD(HD) ensures internal coordination of DOD policy direction, assists SecDef in providing guidance, through the Joint Staff, to combatant commanders for MSCLEA and conducts coordination with DHS. Figure II-2 shows the organizational structure of ASD(HD). The principal duty of ASD(HD) is to provide overall supervision of the HD and CS mission areas within DOD. In that role, ASD(HD) serves as the principal staff assistant and advisor to the USD(P) and Secretary and Deputy Secretary of Defense on HD and CS on matters including, but not limited to:

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

(b) Military support to civil authorities.

(c) Defense Critical Infrastructure Program.

(d) DOD domestic antiterrorism and force protections in accordance with DOD Directive 2000.12.

(e) DOD installation preparedness.

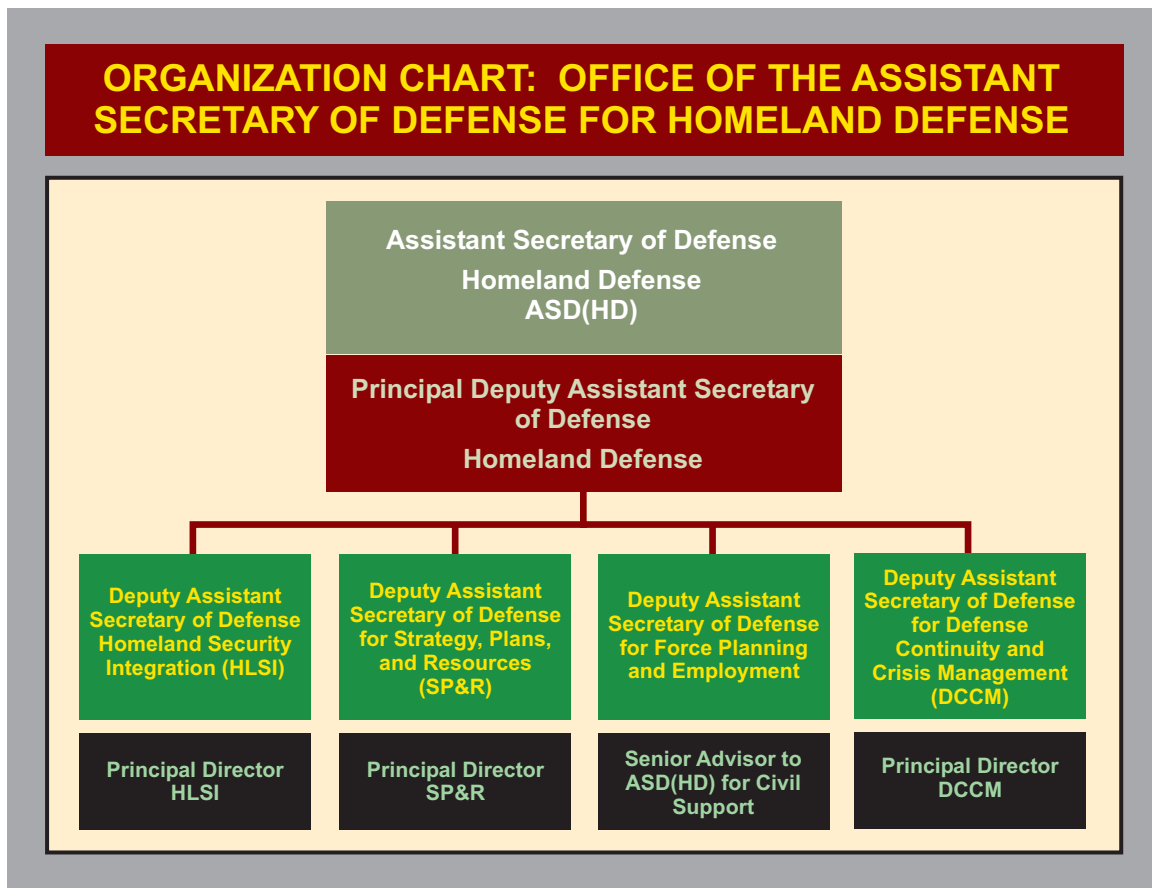
(f) DOD domestic counterterrorism activities, less those involving special operations forces.

(g) DOD continuity-related activities, to include COOP, COG, and Enduring Constitutional Government managed under the Defense Continuity Program.

(h) Domestic crisis management including planning and response to man-made and natural disasters including the consequences of incidents involving weapons of mass destruction.

(i) Policy guidance on homeland defense-related education, training, and professional development programs.





**Figure II-2. Organization Chart: Office of the Assistant Secretary of Defense for Homeland Defense**

(3) **Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict.** ASD(SO/LIC) provides civilian oversight for combating terrorism. This oversight includes supervision of policy, program planning, and allocation and the use of resources. ASD(SO/LIC) also represents SecDef on combating terrorism matters outside DOD.

(4) **Assistant Secretary of Defense for Health Affairs.** ASD(HA) is a critical component in the Services activation of the federal coordinating centers (FCCs). FCCs are DOD and VA medical facilities responsible for locating all civilian beds in their geographic location, arranging the transport of patients from arriving aircraft, and all logistics of receiving mass casualties from a disaster area.

(5) **Assistant Secretary of Defense for Reserve Affairs.** ASD(RA) is responsible for monitoring Reserve Component (RC) readiness. ASD(RA) provides policy regarding the appropriate integration of Reserve and National Guard (NG) forces into HS response efforts.

(6) **Chairman of the Joint Chiefs of Staff.** CJCS has numerous responsibilities relating to HS. These include advising the President and SecDef on operational policies, responsibilities, and programs; assisting SecDef in implementing operational responses to threats or acts of terrorism; and translating SecDef guidance into operation orders to provide assistance to the LFA. CJCS ensures that

HD and CS plans and operations are compatible with other military plans. In the CS mission area, CJCS serves as the principal military advisor to SecDef and the President in preparing for and responding to CBRNE incidents, ensures that military planning is accomplished to support the LFA for CrM and CM, and provides strategic guidance to the combatant commanders for the conduct of CD operations. CJCS also assists combatant commanders in meeting their operational requirements for executing HD missions and for providing CS that has been approved by SecDef. CJCS HD and CS responsibilities include:

- (a) CBRNE/WMD CM.
- (b) Maritime defense and interdiction.
- (c) Air defense.
- (d) Information and intelligence sharing.
- (e) Integrated air, land, and maritime surveillance.
- (f) Mission assurance.
- (g) Biological/chemical defense.
- (h) Combating terrorism.

(7) **Commander, North American Aerospace Defense Command.** By international agreement (The NORAD Agreement and Terms of Reference, and the Canadian/US Basic Security Document 100/35), CDRNORAD leads the bi-national command composed of Canadian and US forces responsible for aerospace control and aerospace warning for North America. North American Aerospace Defense Command's (NORAD's) relationship with USNORTHCOM is unusual in that while they have separate missions defined by separate sources, most of USNORTHCOM's AOR overlaps with NORAD's operational area. NORAD and USNORTHCOM are two separate commands, and neither is subordinate to the other or a part of the other, but they work very closely together. Members of the two commands work side-by-side within the Cheyenne Mountain Operations Center (CMOC) and, in many cases, United States personnel are dual-hatted in positions on both staffs.

(8) **Commander, US Northern Command.** CDRUSNORTHCOM has specific responsibilities for HD and for assisting civil authorities. USNORTHCOM's mission is to conduct operations to deter, prevent, and defeat threats and aggression aimed at the United States, its territories, and interests within the assigned AOR and as directed by the President or SecDef, provide military assistance to civil authorities including CM operations. USNORTHCOM embodies the principles of unity of effort and unity of command as the single, responsible, designated DOD commander for overall C2 of DOD support to civil authorities within the USNORTHCOM AOR. CDRUSNORTHCOM takes all operational orders from and is responsible to the President through SecDef.

(a) **Organization and Command Relationships.** The command organizes and executes its missions with forces assigned by the “Forces for Unified Commands” memorandum and designated functional components under its COCOM. In providing CS, the command may operate through subordinate joint task forces (JTFs). Forces required in support of HD and CS mission areas are provided through the request for forces process per CJCS Manual 3122.01A, *Joint Operation Planning and Execution System, Volume I (Enclosure R)*.

(b) **CDRUSNORTHCOM is the supported commander responsible for conducting HD operations within its AOR.** CDRNORAD conducts aerospace warning and aerospace control missions for North America per NORAD Agreement and Terms of Reference. Air operations performed within USNORTHCOM’s AOR that do not fall within these NORAD mission areas or NORAD’s operational area, or are unilateral (US-only) operations in CONUS or Alaska, will be accomplished through CDRUSNORTHCOM. When directed by the President, CDRUSNORTHCOM is responsible for conducting military operations within the homeland utilizing forces to deter, prevent, or defeat an incursion of sovereign territory.

(c) **Within the designated AOR, CDRUSNORTHCOM is the DOD principal designated agent and the supported commander for the HD and CS mission areas.** The command receives requests for military assistance in support of civilian authorities in accordance with current DODDs.

**1. Standing Joint Force Headquarters — North (SJFHQ-N).** A standing joint force headquarters is a full-time joint C2 element within the geographic combatant commander’s staff that has a daily focus on warfighting readiness and is a fully integrated participant in the commander’s staff planning (deliberate and crisis) and operations. It provides the commander with a trained and equipped standing joint C2 capability specifically organized to conduct planning and develop enhanced situational understanding within a commander-designated focus area. When directed by SecDef to conduct an HD or CS mission, CDRUSNORTHCOM can deploy SJFHQ-N to enable the rapid stand-up of a JTF headquarters.

**2. Joint Task Force — Civil Support (JTF-CS).** JTF-CS plans and integrates DOD support to the designated LFA for domestic CBRNE CM operations. When directed by SecDef, CDRUSNORTHCOM deploys JTF-CS to CBRNE incident sites, establishes C2 of designated DOD forces, and provides MACA.

**3. Joint Task Force — North (JTF-N).** JTF-N detects, monitors, and supports interdiction of suspected transnational threats within and along the approaches to CONUS; fuses and disseminates intelligence, contributes to the COP and coordinates support to LFAs; and supports security cooperation initiatives in order to secure the homeland and enhance regional security.

**4. Joint Force Headquarters — National Capital Region (JFHQ-NCR).** JFHQ-NCR plans, coordinates, and maintains situational awareness, and as directed, employs forces for HD and MACA in the National Capital Region’s operational area to safeguard the Nation’s capital.



*Commander, US Northern Command is responsible for conducting combat operations within the homeland utilizing forces to deter, prevent, or defeat an incursion of sovereign territory.*

Note: There are special circumstances when the President and the governor of an affected state both authorize a state National Guard commander to be placed on Title 10 status and retain Title 32 authority. In this case, Title 10 forces may be placed under the control of this commander who reports to both the governor (for state requirements) and the supported combatant commander (for DOD mission assignments) through an interplay of 32 USC 315 and 325 and 10 USC 104.

(9) **Commander, US Pacific Command.** CDRUSPACOM has specific responsibilities for HD and for assisting civil authorities within the assigned AOR. USPACOM's mission is to conduct operations to deter, prevent, and defeat threats and aggression aimed at the United States, its territories, and interests within the assigned AOR and, as directed by the President or SecDef, provide MACA including CM operations. CDRUSPACOM, as the single responsible commander, embodies the principles of unity of effort and unity of command and is the designated DOD commander for overall C2 of DOD support to civil authorities within the USPACOMAOR. CDRUSPACOM takes all operational orders from and is responsible to the President through SecDef.

(a) **Organization and Command Relationships.** USPACOM organizes and executes its missions through assigned Service components and designated functional components under its COCOM.

(b) **CDRUSPACOM is responsible for conducting HD operations within its AOR.** When directed by the President, CDRUSPACOM is responsible for conducting combat operations to deter, prevent and defeat an incursion of sovereign territory. Within the designated AOR, CDRUSPACOM is the supported commander for HD, specifically air, land, and maritime missions.

(c) **Within the USPACOM AOR, CDRUSPACOM is the DOD designated planning agent and the supported commander for the HD and CS mission areas.** The command receives requests for military assistance in support of CS in accordance with current DODDs.

(10) **Commander, US Strategic Command.** The mission of US Strategic Command (USSTRATCOM) is to establish and provide global strike and coordinated space and IO capabilities to meet deterrent and decisive national security objectives. USSTRATCOM provides operational space support and specialized planning expertise to the joint warfighter. In addition, CDRUSSTRATCOM serves as the coordinating authority for global missile defense. CDRUSSTRATCOM is responsible for planning, integrating, and coordinating intelligence, surveillance, and reconnaissance (ISR) support of strategic and global operations.

(a) CDRUSSTRATCOM is responsible for the following activities associated with HD:

1. Planning, integrating and coordinating global missile defense operations and support (air, land, maritime, and space-based).

2. Integrating of global strike planning and C2 in support of theater and national objectives. USSTRATCOM will only conduct global strike missions in complete coordination with, and in support of, other combatant commanders unless otherwise directed by the President.

3. Planning, integrating, and coordinating DOD IO that have a trans-regional impact or that directly support national objectives.

4. Planning, integrating, and coordinating intelligence, surveillance and reconnaissance in support of strategic military operations, as directed.

5. Planning and implementing security assistance relating to military space operations, and providing assessments as required.

(b) CDRUSSTRATCOM also serves as the supporting commander to USNORTHCOM and USPACOM for the HD and CS mission areas within their AORs.

(11) **Commander, US Special Operations Command.** CDRUSSOCOM serves as a supported or supporting commander for selected counterterrorism activities and serves as the supporting commander to CDRUSNORTHCOM and CDRUSPACOM within their respective AORs when requirements exceed conventional forces' capabilities and special operations forces expertise is needed. When directed by the President or SecDef, CDRUSSOCOM conducts special operations and provides special operations forces as required in support of the LFA during CS operations. CDRUSSOCOM may also provide liaison officers and other assistance to the supported combatant commanders as required.

(12) **Commander, US Transportation Command.** CDRUSTRANSCOM is a supporting commander and serves as the DOD single manager for transportation, providing common-user air, land, and sea transportation, common-user port management and terminal services to meet national

security objectives. For HD missions, CDRUSTRANSCOM serves as the supporting commander to CDRUSSTRATCOM for designated global strike and selected counterterrorism activities. CDRUSTRANSCOM also serves as the supporting commander to CDRUSNORTHCOM and CDRUSPACOM within their respective AORs for HD and CS mission areas. When directed by the President or SecDef, CDRUSTRANSCOM provides transportation as required in support of the LFA during CS operations.

(13) **Commander, US Joint Forces Command.** CDRUSJFCOM's role in HS is to provide support to other combatant commands in United States Joint Forces Command's (USJFCOM's) role as joint force provider, joint force integrator, joint force trainer, and through joint concept development and experimentation.

(14) **Commander, US Southern Command**

(a) CDRUSSOUTHCOM is a supporting commander to USNORTHCOM for HD. Principal functions include the detection and monitoring of illicit trafficking activities in source and transit zones, FP, combating terrorism, countermigration operations, and DCI protection. To assist in the defeat of illicit trafficking, United States Southern Command (USSOUTHCOM) components conduct surveillance of air and maritime routes to the United States. USSOUTHCOM monitors illicit trafficking and migration operations transiting along the southern avenues of approach into the homeland and provides warning and hand-off of threats to USNORTHCOM.

(b) CDRUSSOUTHCOM serves as a supporting commander to USNORTHCOM and NORAD for HD and CS mission areas for US territories in the Caribbean.

(15) **Commander, US European Command (CDRUSEUCOM).** CDRUSEUCOM is a supporting commander to CDRUSNORTHCOM and CDRUSPACOM for HD. Specifically, United States European Command (USEUCOM) provides a forward presence to obtain information on potential adversaries that may be planning attacks on the homeland. Additionally, USEUCOM provides support to homeland defense missions by denying adversaries air, land, and maritime approaches to the homeland.

(16) **Commander US Central Command (CDRUSCENTCOM).** CDRUSCENTCOM is a supporting commander to CDRUSNORTHCOM and CDRUSPACOM for HD. Specifically, United States Central Command (USCENTCOM) provides a forward presence to obtain information on potential adversaries that may be planning attacks on the homeland. Additionally, USCENTCOM provides support to HD missions by denying adversaries air, land, and maritime approaches to the homeland.

(17) **Reserve Component Forces.** NG and Reserve forces are collectively referred to as RC forces and are integral to the accomplishment of peacetime missions and conflict prevention. They are also an essential part of the HS operational force and consist of the Army National Guard (ARNG), the US Army Reserve (USAR), the US Naval Reserve (USNR), the US Marine Corps Reserve (USMCR), the ANG, the US Air Force Reserve (USAFR), and the US Coast Guard Reserve (USCGR). **Guidelines for the utilization of RC forces when called to active duty are found in Title 10 United States Code (USC).**

(a) **Chief, National Guard Bureau (CNGB).** The National Guard Bureau coordinates between DOD and the states/territories, and the District of Columbia on matters pertaining to the NG. The CNGB, under provisions of Title 10, USC Section 10503 is responsible for (not all inclusive):

1. Prescribing the training discipline and training requirements for the ARNG and ANG of the US.

2. Ensuring that units and members of the ARNG and ANG are trained by the states in accordance with approved programs, policies, and guidance from the Secretaries of the Army, Air Force, and the CNGB.

3. Facilitating and supporting the training of members and units of the NG to meet state requirements.

(b) **National Guard.** The NG primarily operates under three different command relationships: federal funding and federal control (10 USC); federal funding and state control (32 USC); and state status (state funding and state control). NG adjutants general and commanders are responsible for planning and training for federal and state missions. The SecDef may provide funds to a governor to employ NG units or members to conduct homeland defense activities that the SecDef determines to be necessary and appropriate for participation by the NG units or members, as the case may be.



*The Department of Defense responds to civil support incidents that require resources beyond the capabilities of local and state-level emergency response organizations.*

1. The NG, when in state status, responds under the governor's control for CS missions in accordance with state laws. However, when NG personnel or units are federalized by order of the President under 10 USC, they respond under the same legal restrictions and C2 structures as active component military forces.

2. **The NG, when in state status, is normally the first military responder to CS incidents that require resources beyond the capabilities of local and other state-level emergency response organizations.** Working under the control of the governor, their actions are closely coordinated with those of other agencies, to include any DOD assets committed to the same or related incidents. Additionally, in many states, the adjutant general is also the state's Director for Emergency Management, and as such, not only controls the response of the state's NG forces, but also manages and coordinates the state's response to CM in support of local governments.

3. **National Guard Weapons of Mass Destruction – Civil Support Teams (WMD-CSTs).** The NG, operating under 32 USC or state status, is likely to be the first military responder to a CBRNE incident site or area. The WMD-CST's mission is to support civil authorities at a domestic CBRNE incident site by identifying CBRNE agents/substances, assessing current and projected consequences, advising on response measures, and assisting with appropriate requests for additional support.

(c) **Reserve Forces.** Each of the seven RCs is structured and operated in a manner similar to its respective Active Component counterpart. Unlike the ARNG and ANG, the remaining five RC organizations (USAR, USNR, USAFR, USMCR, USCGR) operate under the same C2 relationships in both peacetime and wartime and do not have State-specific relationships. When called to active duty, Reserve forces conduct HS missions under Title 10 guidelines exactly as Active Component forces. While on active duty, members of the USAR, USNR, USAFR, USMCR and the USCGR are subject to the provisions of the Uniform Code of Military Justice. Reserve forces are called to active duty through the mobilization/demobilization process.

*For additional information on the RC mobilization/demobilization process, see JP 4-05.1, Joint Tactics, Techniques, and Procedures for Manpower Mobilization and Demobilization Operations: Reserve Component Callup.*

(18) **US Coast Guard. USCG is a Military Service and a branch of the Armed Forces of the United States in DHS (Title 14, USC 1).** When directed by EO of the President or upon declaration of war by Congress, the USCG transfers to the Department of the Navy for operations. In this capacity, the Commandant, USCG reports directly to the Secretary of the Navy (SECNAV) for all matters pertaining to equipping, training and employment of the Service. SECNAV will assume those statutory duties granted to the secretary of the department. However, at any time, USCG may also assist the Navy without transferring forces by attaching units to a Navy command, with the gaining commander exercising TACON of the attached units.

(a) USCG's HS mission is to protect the US maritime domain and the US Marine Transportation System and deny their use and exploitation as a means for attacks on US territory, population and critical infrastructure. Additionally, USCG will prepare for and, in event of attack, conduct emergency response operations.





*The United States Coast Guard is the lead federal agency for maritime security operations for Homeland Security in the US maritime domain.*

(b) USCG is the LFA responsible for the conduct and coordination of maritime security operations carried out under civil authorities for HS in the US maritime domain. When USCG is serving in this role, DOD assets will serve in a supporting role; however, C2 relationships will be tailored to the particular situation. There are situations where USCG is a supporting agency operating in support of other federal, state, and local civil agencies and coordinates its operations, both domestic and foreign, with federal, state and local agencies. In all cases, operations are governed by unity of effort and agreed protocols. **In its maritime law enforcement role, USCG has jurisdiction in both US waters and on the high seas and is the only military service not constrained by the Posse Comitatus Act (i.e., it is unique among the Services in that it has statutory law enforcement authority).**

(c) When elements of USCG are attached to DOD for execution of maritime HD missions, USCG elements will execute those missions assigned by the combatant commander (e.g., USNORTHCOM/USPACOM) and serve as a supporting command. The USCG Atlantic and Pacific area commanders may serve as joint force maritime component commanders for HD.

### **3. Federal Agency Responsibilities and Considerations**

DOD is one of many federal agencies and organizations with HS responsibilities. To facilitate coordination of these various activities and capabilities, there are interagency groups and plans in which DOD is an active participant. Except for HD missions, DOD will serve in a supporting role for domestic incident management.

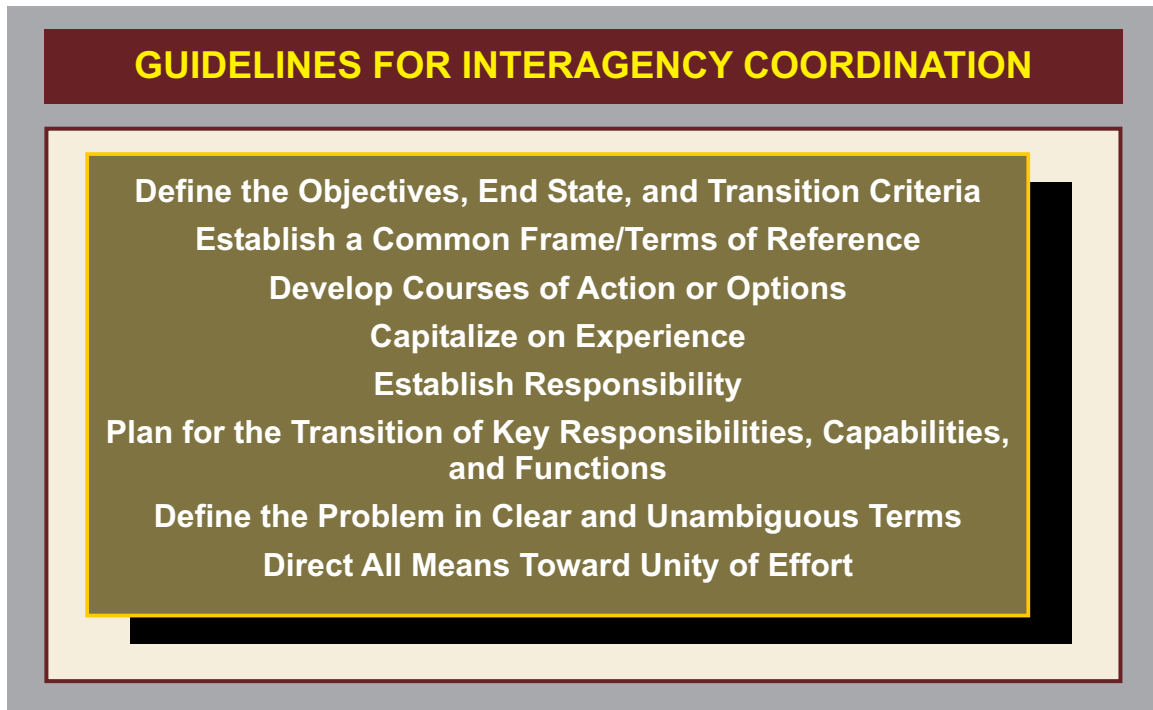
a. **The Interagency Process at the National Level.** The interagency process is grounded within the Constitution and established by law in the National Security Act of 1947. The National Security Act of 1947, as amended, established the NSC to advise the President with respect to the integration of domestic, foreign, and military policies relating to national security. HSPD-1, *Organization and Operation of the Homeland Security Council*, designated the Homeland Security Council (HSC) as the senior forum for HS issues. There are numerous NSC and HSC policy-coordinating committees that have HS responsibilities.

*See HSPD-1, Organization and Operation of the Homeland Security Council, for more information.*

b. **Interagency Guidelines.** Working in concert forges the vital links between the military instrument of national power and the economic, diplomatic and informational instruments of the US Government. Synchronization and integration of all instruments of national power are required to ensure the successful execution of HS missions. The challenges facing the Nation are increasingly complex and will require the skills and resources of many organizations. Figure II-3 is a synopsis of the guidelines listed below. Guidelines for interagency coordination include:

- (1) Achieve unity of effort among a mix of federal, state and local agencies.
- (2) Identify all agencies and organizations potentially involved in the operation.
- (3) Identify key elements of information that various agencies can share.
- (4) Establish an interagency hierarchy for the response effort.
- (5) Identify appropriate resources of each participant.
- (6) Define the objectives of the response effort.
- (7) Define the desired end state and exit criteria.
- (8) Define courses of action for the supporting effort.
- (9) Identify potential obstacles.
- (10) Maximize the mission's assets to support long-term goals.
- (11) Establish interagency assessment teams.

*See JP 3-08, Interagency Coordination During Joint Operations, and National Security Presidential Directive (NSPD) 1, Organization of the National Security Council System, for more information.*



**Figure II-3. Guidelines for Interagency Coordination**

c. HD and CS mission areas require detailed planning and interagency coordination to develop operational relationships with other federal departments and agencies. In certain circumstances DOD's dependence on non-DOD organizations, information, assets and infrastructures could be critical in the accomplishment of HD as well as CS mission areas. **ASD(HD) is responsible for coordinating all HD and CS mission area matters with other executive departments and federal agencies.** ASD/HD will ensure that DOD strategy is consistent with and fully supports the NSHS effort.

d. **All combatant commanders have permanently assigned joint interagency coordination groups (JIACGs).** JIACGs assist the combatant commanders by providing interagency support of command plans, operations, contingencies, exercises and initiatives, all in support of assigned mission responsibilities. The goal of a JIACG is to provide timely, usable information and advice from an interagency perspective to the combatant commander, by information sharing, integration and synchronization, and training and exercising. JIACGs may include representatives from other Federal departments and agencies and state and local authorities, liaison officers (LNOs) from other commands and DOD components, and the assigned support staff for the JIACG. The representatives and LNOs are the subject matter experts for their respective agencies and commands, and provide the critical bridge between the combatant commander and the appropriate LFA as required.

*For additional information see JP 3-08, Interagency Coordination During Joint Operations.*

e. **Interagency Plans.** Given the complexity and extent of federal, state, and local participation in domestic incident management, there are various operational national-level plans and agreements that depict the roles and responsibilities of participants in different incident management and emergency response circumstances. The NRP provides a "National framework" for integrating various plans and organizations involved in crisis planning and response.

#### 4. Non-Department of Defense Federal Agencies and Responsibilities

DOD is the lead for HD missions and will be supported by other federal agencies for such missions. An agency other than DOD will be supported for CS missions and DOD will play a role in providing that support. Figure II-4 reflects this relationship.

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

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

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



Figure II-4. Lead Federal Agency/Department of Defense Relationships

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

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

**b. The Department of Homeland Security. The Homeland Security Act of 2002 established this department with five distinct directorates and two independent Services — the Secret Service and the Coast Guard.** Figure II-5 shows the organizational structure of DHS. Each of the five directorates is discussed below.

(1) **The Border and Transportation Security (BTS) Directorate** is responsible for securing the nation's borders and transportation systems, and for enforcing our immigration laws. The Bureau of Immigration and Customs Enforcement, Bureau of Customs and Border Protection, the Animal and Plant Health Inspection Service, the Federal Protective Service, Office for Domestic Preparedness, and the Transportation Security Administration are elements of this directorate. The Federal Protective Service is assigned the role of protecting government buildings — a task closely related to DHS's infrastructure protection responsibilities. BTS ensures all aspects of border control, including the issuing of visas, and is kept informed by a central information-sharing clearinghouse and compatible databases.

(2) **The Emergency Preparedness and Response Directorate** oversees Federal government assistance in the domestic disaster preparedness training of first responders and coordinates the government's disaster response efforts. The Federal Emergency Management Agency (FEMA) is the primary agency operating in support of this directorate. It manages critical response assets such as the Nuclear Emergency Search Team (Department of Energy) and the Strategic National Stockpile (Health and Human Services). This directorate integrates the federal interagency emergency response plans into a single, comprehensive, government-wide plan, and ensures that all response personnel have the equipment and capability to communicate with each other as necessary.

(3) **The Science and Technology Directorate** is the primary research and development arm of the DHS. It organizes the scientific and technological resources of the United States to prevent or mitigate the consequences of attacks on the nation. The Directorate also sponsors research, development, and testing; and invents new vaccines, antidotes, diagnostics, and therapies against biological and chemical agents.

(4) **The Information Analysis and Infrastructure Protection Directorate** analyzes intelligence and other information pertaining to threats to the homeland. It draws from multiple sources — including the Central Intelligence Agency (CIA), National Security Agency (NSA), FBI, Bureau of Immigration and Customs Enforcement, Drug Enforcement Administration (DEA), Department of Energy (DOE), Customs, Department of Transportation, and data gleaned from other organizations. This directorate provides the capability to identify and assess current and future threats to the homeland, maps threats against current vulnerabilities, issues timely warnings, and immediately takes appropriate preventive and protective action. The directorate also evaluates the vulnerabilities of America's critical infrastructure, including food and water systems, agriculture, health systems and emergency services, information and telecommunications, banking and finance, energy (electrical, nuclear,

## DEPARTMENT OF HOMELAND SECURITY

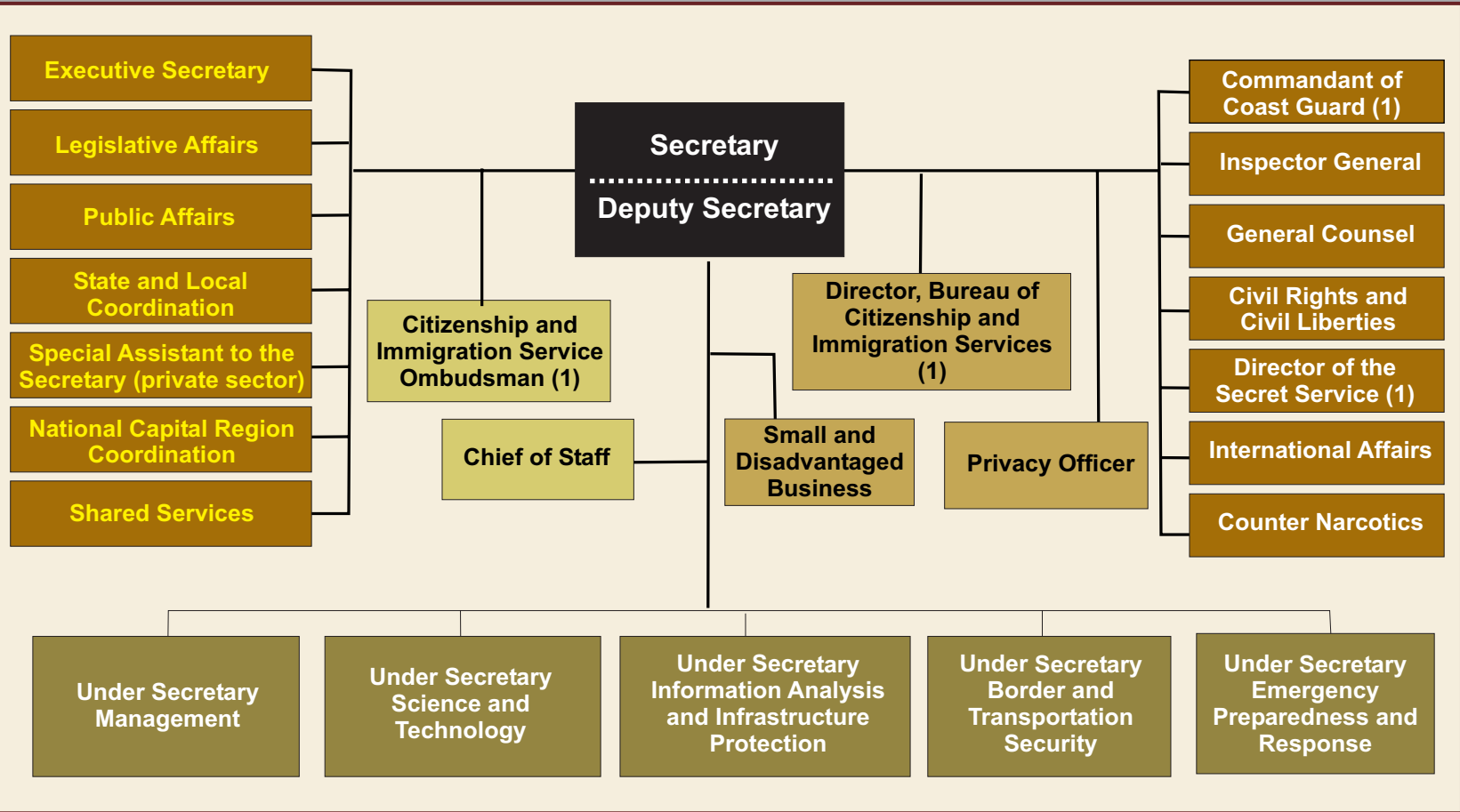


Figure II-5. Department of Homeland Security

gas and oil, dams), transportation (air, road, rail, ports, waterways), the chemical and defense industries, postal and shipping entities, and national monuments and icons. Overall, the directorate consolidates and streamlines relations within the Federal government for America's state and local governments.

(5) **The Management Directorate** is responsible for budget, management and personnel issues associated with HS.

(6) **The United States Secret Service** is one of two agencies that transferred intact to DHS. The primary mission of USSS is to protect the President and other government leaders. The agency provides security for designated national events, and preserves the integrity of the nation's banking and finance infrastructures. However, it will now do so with the added efficiency of access to DHS intelligence analysis and coordination with other key agencies. Economic security is a key factor in HS. USSS counters criminals and terrorists who attempt to use identity theft, telecommunications fraud, and other technology-based crimes to defraud and undermine American consumers and industry.

c. **Department of Energy.** DOE serves as a support agency to the FBI for technical operations and a support agency to DHS/FEMA for CM. DOE provides scientific and technical personnel and equipment in support of the LFA during all aspects of WMD incidents. DOE assistance can support both CrM and CM activities with capabilities such as threat assessments, domestic emergency support team (DEST) deployment, LFA advisory requirements, technical advice, forecasted modeling predictions, and assistance in the direct support of operations. Deployable DOE scientific technical assistance and support includes capabilities such as search operations; access operations; diagnostic and device assessment; radiological assessment and monitoring; identification of material; development of federal protective action recommendations; provision of information on the radiological response; render safe operations; hazards assessment; containment, relocation and storage of special nuclear material evidence; post-incident cleanup; and on-site management and radiological assessment to the public, the White House, and members of Congress and foreign governments. All DOE support to a federal response will be coordinated through a senior DOE official.

d. **Department of Justice (DOJ)/FBI.** As the lead for crisis management and counterterrorism, the Attorney General is responsible for ensuring the development and implementation of policies directed at preventing terrorist attacks domestically, and will undertake the criminal prosecution of acts of terrorism. DOJ has charged the FBI with execution of its LFA responsibilities for the management of a federal response to threats or acts of terrorism that take place within US territory or those occurring in international waters that do not involve flag vessels of foreign countries. As LFA, the FBI will implement a federal CrM response, and will designate a federal on-scene commander to ensure appropriate coordination with federal, state and local authorities until such time as the Attorney General finds it necessary to transfer the overall LFA role to DHS/FEMA.

e. **Environmental Protection Agency (EPA).** EPA serves as a support agency to the FBI for technical operations, and a support agency to DHS/FEMA for CM. EPA provides technical personnel and supporting equipment to the LFA during all aspects of WMD incidents. EPA assistance may include threat assessment; DEST and regional emergency response team deployment; LFA advisory requirements, technical advice, and operational support for chemical, biological, and radiological releases; consultation;

agent identification; hazard detection and reduction; environmental monitoring; sample and forensic evidence collection/analysis; identification of contaminants; feasibility assessment; clean-up; and on-site safety, protection, prevention, decontamination, and restoration activities. EPA and USCG share responsibilities for response to oil discharges into navigable waters and releases of hazardous substances, pollutants, and contaminants into the natural and physical environment. EPA provides the pre-designated federal on-scene coordinator for inland areas while USCG coordinates resources for the containment, removal, and disposal activities and resources during an oil, hazardous substance, or WMD incident in coastal areas.

f. **Department of Health and Human Services (DHHS).** DHHS assistance supports threat assessment, DEST deployment, epidemiological investigation, LFA advisory requirements, and technical advice. Technical assistance to the FBI may include identification of agents, sample collection and analysis, on-site safety and protection activities, and medical management planning. DHHS serves as a support agency to the FBI for technical operations, and a support agency to DHS/FEMA for CM. DHHS provides technical personnel and supporting equipment to the LFA during all aspects of an incident. DHHS can also provide regulatory follow-up when an incident involves a product regulated by the Food and Drug Administration. Operational support to DHS/FEMA may include mass immunization, mass prophylaxis, mass fatality management, pharmaceutical support operations (Strategic National Stockpile), contingency medical records, patient tracking, and patient evacuation and definitive medical care provided through the National Disaster Medical System.

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

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

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

## 5. Special Considerations

a. When situations are beyond the capability of the state, the governor may request federal assistance from the President. The President may direct the Federal Government to provide supplemental assistance to state and local governments to alleviate the suffering and damage resulting from disasters or emergencies. **DHS/FEMA has the primary responsibility for coordination of federal assistance to state and local governments in these instances.**



b. **Specific approval authority for the use of DOD assets is designated by SecDef.** This approval authority applies in the case of sensitive support requests, threats and acts of terrorism, and requests for support from civilian law enforcement authorities that have the potential for confrontation with individuals or groups that may result in the use of lethal force.

c. **Federal agencies may request DOD support based on interagency memoranda of agreement (MOAs).** For example, under an interagency MOA, the US Navy may deploy oil containment and recovery equipment to support USCG (DHS) efforts to clean up oil spills. Interagency MOAs provide the basis for coordinated responses when situations warrant. Interagency and Service MOAs must be reviewed and approved by the DOD Office of the General Counsel.

## CHAPTER III HOMELAND DEFENSE

*“America will not abdicate its freedom and security to anyone or any nation — ever. Instead, as many an enemy has discovered, we will meet the threat of terrorism wherever it seeks to hide, be it on foreign soil or our own.”*

**Secretary of Homeland Security Tom Ridge  
Remarks at the Federal Law Enforcement Training Center  
25 March 2004**

### 1. General

a. DOD HD mission area military capabilities are used to counter threats and aggression against the United States. HD is the responsibility of DOD. It is a layered defense in depth that begins overseas far from the homeland before threats are at our borders. **DOD is the lead, supported by other agencies, in defending against traditional external threats/aggression (e.g., air and missile attack).** However, against internal asymmetric, non-traditional threats (e.g., terrorism), DOD may be in support of DHS and other Federal agencies. **When ordered to conduct HD operations within US territory, DOD will coordinate closely with other federal agencies or departments.** Consistent with laws and policy, the Services will provide capabilities to support combatant command requirements against a variety of air, land, maritime, space, and cyber incursions that can threaten national security. These include air, land, and maritime attacks and threats against critical infrastructure. The purpose of HD is to protect against and mitigate the impact of incursions or attacks on sovereign territory, the domestic population, and DCI. The following goals guide the DOD HD mission area:

- (1) Identify the threat.
- (2) Dissuade adversaries from undertaking programs or conducting actions that could pose a threat to the US homeland.
- (3) Ensure defense of the homeland and denying an adversary’s access to the nation’s airspace, land, and maritime approaches.
- (4) Ensure access to space and information.
- (5) Ensure availability of DCI.
- (6) Deter aggression and coercion by deploying forward with the capability to prevent attacks on the homeland and impose severe penalties for aggression on an adversary’s military capability and supporting infrastructure.
- (7) Decisively defeat any adversary if deterrence fails.
- (8) Minimize the consequences of any attack or incident.

b. **Operations Outside the Homeland.** Outside of the US (in the forward regions and approaches), DOD conducts HD by preventing and denying adversaries access to the nation’s air, land, and maritime approaches. It includes activities that secure our freedom to operate in space and ability to access information. DOD supports HD by global campaigns and operations to disrupt and defeat terrorists before they are able to launch an attack within the US homeland. Finally, DOD security cooperation initiatives foster positive working relationships and interoperability with friends and allies.

c. **Military Activities Within the Homeland.** Operations are conducted within the land, airspace, and territorial waters of the US. These activities require freedom of information and access to space. Operations may include protection of DCI, air and maritime interception, and others.

## 2. Homeland Defense Operational Elements and Characteristics

a. DOD HD missions are conducted in accordance with the law, National, DOD, CJCS, joint, Military Department, and Military Service policy, directives, doctrine and tactics, techniques, and procedures. **HD missions are conducted through a combination of offensive actions and active and passive defenses.** Figure III-1 is a graphic depiction of the HD missions' operational elements and enablers.

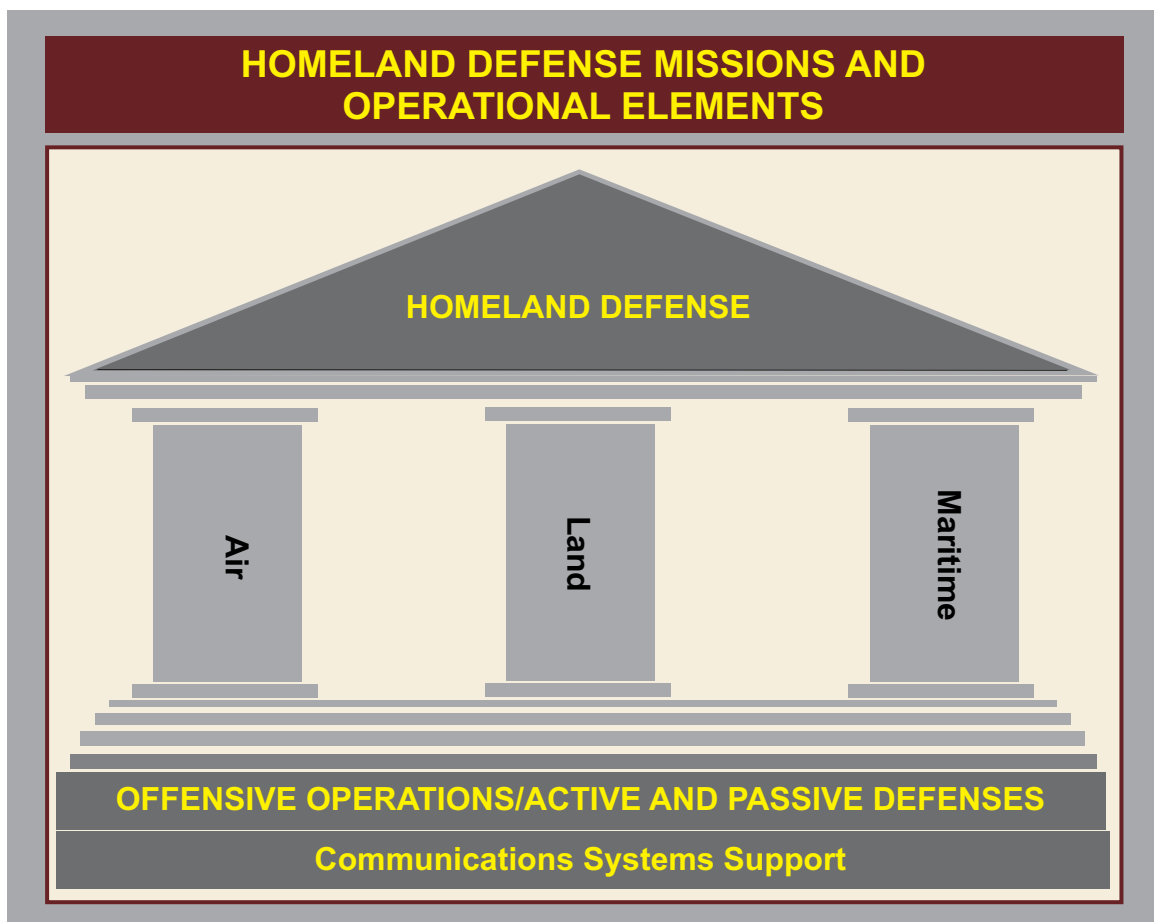


Figure III-1. Homeland Defense Missions and Operational Elements

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

c. **Deterring adversaries is a key HD objective and DOD EP activities, coupled with offensive and defensive capabilities, may deter an adversary from threatening or attacking the homeland.** Well-trained, rapidly deployable forces conducting realistic exercises are but one example of actions and capabilities that may serve as a deterrent.

d. **If deterrence fails, DOD must be prepared to rapidly respond and defend against threats and aggression.** DOD, as directed by the President, may conduct preemptive/offensive HD actions in accordance with international and domestic law, national policy, and directives. The objective of these operations is to destroy, degrade, disrupt, or neutralize weapons, launch platforms, supporting command, control, and communications, logistics and ISR capabilities before they are employed by an adversary. Air, land, sea, space, and special operations forces may conduct offensive actions. Examples of offensive operations may include global strikes. Global strikes may be described as rapidly planned, limited-duration, extended-range precision attacks that are conducted to achieve strategic objectives. They may be executed against highly valued adversary assets using lethal and nonlethal methods. Targets include adversary centers of gravity; WMD, their delivery systems, production facilities, and storage sites; key leadership; and critical infrastructure. Other examples of HD offensive actions include direct action, space denial, and computer network attack. Offensive actions may be preemptive in nature.

e. **Primary defensive actions associated with HD missions include active and passive defense measures.** The objective of HD active defenses is to defeat threats that are already deployed or en route to the target. Active defenses are layered, deployed in depth, and are designed to destroy, nullify, or reduce the effectiveness of attacks on our sovereign territory, domestic population, and DCI employing kinetic and non-kinetic weapons capabilities. Active defenses employ air, land, sea, space, and special operations forces. Defenses may also include offensive IO capabilities to disrupt adversary information systems. The objective of HD passive defense is to reduce the probability of, and minimize the damage caused by, hostile actions. Passive defenses include FP and critical infrastructure risk mitigation actions to reduce targeting effectiveness. They are normally developed and executed throughout the defending force. Passive defense measures include selected FP actions, deception, mobility, dispersion, systems hardening and protective construction, strategic, operational, and tactical warning and surveillance, operations security (OPSEC), and recovery and reconstitution efforts.

f. **Communications systems are key to all HD offensive and defensive operations.** Communications systems enable centralized planning and the coordinated and mutually supporting employment of forces and assets. A COP facilitates decentralized execution in rapidly changing operational environments. Intelligence, logistics, and operations information must be shared among appropriate

agencies, to include law enforcement, when building the COP. Communications systems and architectures also provide commanders with the capabilities necessary to plan missions, control and direct forces, and coordinate and execute operations. **Effective communication systems for air, land, and maritime defenses should be capable of rapidly exchanging information as well as displaying information of common concern.** The information exchange between all levels of command should be redundant and flexible even when an intermediate level has been disabled. These systems include command centers, operations centers, processing centers and systems, and data sources and communications systems. An example of a critical communications systems asset is NORAD's warning and assessment capabilities used to support the integrated tactical warning/attack assessment process. Within NORAD's CMOC, the commands involved in the homeland air defense mission (USNORTHCOM, NORAD, USPACOM and USSTRATCOM) share selected communications systems and architecture which enables effective coordination, synchronization, integration, and seamless defenses.

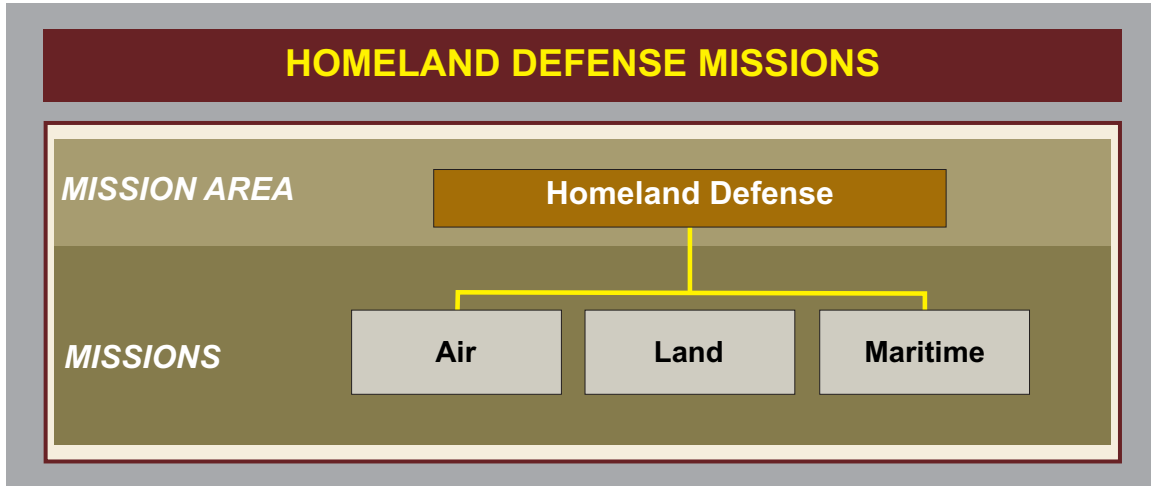
### 3. Homeland Defense Missions

a. **The joint force HD mission area encompasses three broad missions: the air mission, the land mission, and the maritime mission.** When directed by the President and SecDef, DOD conducts HD missions in defense of our population, sovereign territory and NCI & KA. The survival and security of the US will likely depend on the effective employment of defenses in depth to destroy or defeat a variety of threats. The USNORTHCOM and USPACOM commanders are responsible in their respective AORs for the homeland air mission, land mission, and maritime mission. NORAD is charged with aerospace warning and aerospace control for North America. Aerospace warning includes the monitoring of manmade objects in space, and the detection, validation, and warning of attack against North America whether by aircraft, missiles, or space vehicles, using mutual support arrangements with other commands. Aerospace control includes providing surveillance and control of Canadian, US, Puerto Rico, and US Virgin Islands airspace.

b. Selected HD missions and operations will require extensive integration and synchronization and may also overlap and occur simultaneously. **In addition, HD missions may transition to one or more types of CS.** For example, attacks on the homeland intended to destroy NCI&KA could cause mass evacuation and relocation of civilians in addition to extensive casualties. In this instance, while executing offensive HD operations and active defense to defeat the threat, DOD may be required to assist civil authorities in mitigating the consequences of previous attacks that partially disrupted or destroyed their intended targets. Figure III-2 depicts the three HD missions (air, land, and maritime).

c. The following outlines and describes the missions associated with homeland defense:

(1) The HD air mission includes all measures taken to deter, detect, or destroy hostile air threats against the US homeland. Air defenses are designed to destroy, nullify, or reduce the effectiveness of attacking adversary aircraft, and manned and unmanned missiles. **No single action is capable of providing complete protection from a coordinated air attack and a combination of offensive operations and active and passive defense measures will be required.**



**Figure III-2. Homeland Defense Missions**

(2) Land missions include HD operations taken under extraordinary circumstances to deter, and if necessary, defeat land threats when the President directs or SecDef orders. Although the threat of a full-scale land invasion by a hostile power is remote, when directed by the President, ground forces may be employed to conduct offensive HD operations and establish active and passive defenses in depth to counter a host of conventional and asymmetric threats.

(3) Maritime missions include HD operations taken to detect, deter, defeat, or nullify maritime threats against US territory, domestic population and infrastructure. A full-scale maritime invasion of the homeland is also unlikely, but when directed by the President, maritime forces may be employed to conduct offensive HD operations and active and passive defenses in depth to counter maritime attacks within US territorial waters. However, maritime missions are conducted globally that contribute to homeland defense.

*When published detailed information concerning HD operations will be contained in JP 3-26.1, Joint Doctrine for Homeland Defense.*

#### **4. Supporting Operations and Enabling Activities**

a. **HD supporting operations and enabling activities include CIP, space operations, AT and FP activities, BMD, and IO.** Supporting operations and enabling activities should be considered in the planning and execution of all aspects of HD. HD supporting operations and enabling activities often overlap with one another and specific tasks may be closely related. For example, when performing activities associated with protecting DCI (a key fuel line), planners must also consider AT and FP measures to protect Service members or specific facilities and equipment. Continued operation of information systems deemed vital to C2 (computer network defenses and information assurance [IA] activities) will also be required.

b. The following describes the HD supporting operations and enabling activities identified above and how they may be applied across HD missions.

(1) **Critical Infrastructure Protection.** CIP activities consist of the identification, prioritization, assessment, and security enhancement of infrastructure network assets essential to mobilize, deploy, and sustain DOD military operations. **DCI generally consists of physical (installations, power projection platforms, etc.), and nonphysical (electronic information) assets.** The increasing interconnectivity and interdependence among commercial and defense infrastructures demand that DOD also take steps to understand the vulnerabilities of, and threats to, the critical infrastructures on which it depends for mission assurance. The DCIP is a fully integrated program that provides a comprehensive process for understanding and protecting selected infrastructure assets that are critical to national security during peace, crisis, and war. It involves identifying, prioritizing, assessing, protecting, monitoring, and assuring the reliability and availability of mission-critical infrastructures essential to the execution of the NMS. The program also addresses the operational decision support necessary for combatant commanders to achieve their mission objectives despite the degradation or absence of these infrastructures.

*For more information concerning CIP and the DCIP see DODD 3020, Defense Critical Infrastructure Identification, Prioritization, and Protection Defense Critical Infrastructure Program (DCIP).*

(a) **DOD serves as LFA to prepare for, respond to, and defend against adversary attacks on DCI.** USD(P) acts as the principal staff assistant and civilian advisor to SecDef on DCIP activities and provides policy and strategy guidance. CJCS is the principal military advisor to the SecDef on DCIP activities and is responsible for the assessment(s), coordination, integration prioritization, and guidance for DOD CIP operations. Under the role of force protection, geographic combatant commanders and Service Chiefs are responsible for operational assessments, planning, integration, and protections of DCI.

(b) **Combatant commanders conducting HD missions are responsible for establishing CIP programs that conform to DOD requirements and policy.** DOD components are also responsible for establishing CIP programs. The components must identify and assess the critical assets and infrastructure dependencies that are necessary for the successful execution of present and projected military operations, their fulfillment of homeland defense missions, and protection of US interests at home. Components also address CIP issues at the installation level.

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

(2) **Space Operations.** The region of space above the US cannot be owned or possessed like territory. It is US Government policy, however, that purposeful interference with US space systems will be viewed as an infringement on the Nation's sovereign rights. **In order to deter or preempt attacks and protect our military space assets, DOD conducts space operations in support of HD missions, through space control, space force enhancement, and space support mission areas.** DOD CIP activities may be closely related to military space operations, given that selected space capabilities may be classified as DCI. For HD missions, CIP activities may serve to protect and

defend our abilities 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. CDRUSSTRATCOM is also responsible for CIP activities associated with DOD IO, which includes computer network operations (CNO). CDRUSSTRATCOM may also conduct space operations and IO as a supporting commander to CDRUSNORTHCOM or CDRUSPACOM in the performance of their HD missions.

*For more information concerning space and information operations see JP 3-14, Joint Doctrine for Space Operations, and JP 3-13, Joint Doctrine for Information Operations.*

(3) **Antiterrorism and Force Protection.** DOD AT and FP programs are interrelated and should be applied and integrated across the entire HD mission area. FP is an overarching mission that ties together the DOD mission assurance functions. FP activities include actions taken to prevent or mitigate hostile actions against DOD personnel (including family members), resources, facilities, and critical information. Activities contributing to the FP mission include AT, CIP, COOP, logistics, medical, legal, and safety. DOD's AT program is one of several security programs that serve as key elements of DOD's combating terrorism and FP efforts. DOD AT activities focus on collective proactive efforts to detect and prevent terrorist attacks against DOD personnel, their families, facilities, installations, and non-CIP infrastructure critical to mission accomplishment. **DOD AT activities focus on collective proactive efforts to detect and prevent terrorist attacks against DOD personnel, their families, facilities, installations, and infrastructure critical to mission accomplishment.** The minimum elements of an AT program are AT risk management, planning, training and exercises, resource generation, and program review. DOD programs assume that threat actors exist and possess the capability and intent to attack our assets and interests. Effective and integrated AT and FP measures are a critical part of our defense against asymmetric threats, and they are key to deterring, preventing, and defeating threats and aggression aimed at DOD installations, assets, personnel, information, and infrastructure. In the defense of the homeland, CDRUSNORTHCOM and CDRUSPACOM are responsible for establishing and validating AT and FP criteria, setting standards for readiness, and establishing readiness levels within their respective AORs. Combatant commanders with functional responsibilities establish AT and FP command policies for the protection of all assigned forces. In accordance with SecDef guidance, CDRUSNORTHCOM exercises TACON for DOD FP and has overall DOD AT program and FP responsibility in CONUS. CDRUSNORTHCOM will not use the authority to move DOD personnel unless faced with a time critical event involving potential loss of life, or personnel movement is required to prevent significant damage to mission critical infrastructure. CDRUSNORTHCOM will notify SecDef immediately of such time critical personnel movements. CDRUSNORTHCOM will seek SecDef approval of pending baseline force protection condition changes no later than 24 hours prior to implementation or as soon as practicable if faced with a critical event. (Note: Detailed guidance for the implementation of CONUS FP measures will be addressed in JP 3-26.1, *Joint Doctrine for Homeland Defense*, and will take into account the unique nature of the homeland and any operational and legal restrictions associated with the guidance in current implementing documents.)

*For more information on DOD AT and FP programs refer to DODD 2000.12, DOD Antiterrorism Program, 18 August 2003; Department of Defense Instruction (DODI) 2000.16, DOD Antiterrorism Standards, 14 June 2001, and JP 3-07.2, Joint Tactics, Techniques, and Procedures for Antiterrorism.*





*Department of Defense antiterrorism activities focus on collective proactive efforts to detect and prevent terrorist attacks.*

(4) **Ballistic Missile Defense.** BMD is a supporting HD mission and its capabilities are designed to detect, deter, defend against, and defeat adversary ballistic missile threats. BMD of the homeland includes the integration of capabilities to destroy or disrupt adversary missiles in flight or prior to launch. BMD consists of sensors, weapons, C2, manning, and logistic systems, which are employed collectively. BMD should fully synchronize and integrate offensive and defensive actions and supporting systems to achieve unity of effort. BMD activities may also be closely related to DOD CIP and FP actions. For example, there may be a requirement to establish a missile defense umbrella over a site that is designated as DCI (e.g., a CONUS POE). Space operations and IO are also 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. Within their respective AORs, CDRUSNORTHCOM and CDRUSPACOM are responsible for conducting homeland BMD while CDRUSSTRATCOM is responsible for planning, integration, and coordination of global missile defense operations and support.

*For more information regarding BMD of the homeland see National Security Presidential Directive (NSPD)-23, 16 Dec 02; and the Unified Command Plan (UCP) 10 January 03.*

(5) **Information Operations.** IO is a critical HD enabler and should always be integrated when planning and executing HD missions. Offensive IO activities within the US and its territories or against US persons are not conducted unless ordered by the President. However IO activities should always be considered when conducting homeland air missions,

land missions, and maritime missions. It must be noted that many policy documents discuss cyber defenses associated with HD, but in accordance with joint doctrine on the subject, ‘cyber attack’ and ‘cyber defense’ are interpreted and applied operationally as CNO. CNO consists of computer network attack and computer network defense and is categorized as a core activity of IO. Additionally, IO core and related activities may overlap or become elements of other missions supporting HD. For example, the requirement to protect critical DOD assets and infrastructure spans IO capabilities associated with CNO. Computer network defense in turn may be a critical element of DCI protection. IO capabilities and activities also serve as critical enablers to our ability to successfully perform missions associated with HD. For example, FP actions may include installation OPSEC and IA measures, which are categorized as core and supporting IO capabilities. Other critical IO that may be used when conducting HD offensive and defensive operations include electronic warfare, PSYOP, and military deception. Physical security is a supporting activity associated with IO that should be considered when conducting HD. CDRUSNORTHCOM and CDRUSPACOM conduct IO within their respective AORs for HD and fully coordinate and integrate their efforts with CDRUSSTRATCOM who has the overall responsibility for integrating and coordinating DOD IO.

*For more information concerning IO see JP 3-13, Joint Doctrine for Information Operations.*

## 5. Planning Considerations for Homeland Defense Operations

When directed, DOD conducts HD activities in accordance with the UCP, appropriate operation plans in concept format (CONPLANS), DODDs, and SecDef strategic guidance statements. Command relationships will be specified in appropriate plans and orders.

a. **Operations.** As with other joint operations, all HD operations are conducted in accordance with doctrine and policy. The campaigns may be designed utilizing the notional campaign phases outlined in JP 3-0, *Doctrine for Joint Operations*, and JP 5-00.1, *Joint Doctrine for Campaign Planning*. Although commanders will determine the actual phases used during a campaign, use of the phases — deter/engage, seize the initiative, decisive operations, and transition, provides a flexible planning model to arrange HD operations.

b. **Simultaneous Operations.** HD missions and common functions may take place simultaneously with other operations to include a CS mission area. **HD operations are conducted across the range of military operations and, unless otherwise directed by SecDef, HD missions will take precedence over CS missions.** Consequently, there may be competing requests for units and support such as transportation, equipment, logistics, and other capabilities that must be balanced against commitments in other theaters. Asset-resourcing conflicts must be quickly coordinated and resolved to prevent delays in responding to time-sensitive requirements.

c. **Public Affairs (PA).** HD missions will draw extensive media attention. Military PA activities are subject to approval of SecDef or the appropriate combatant commander. The Assistant Secretary of Defense for Public Affairs approves and disseminates PA guidance, PA plans, and PA annexes. Commanders make decisions in an operational environment of complex information demands. A number of news media may already be in an operational area when military forces conduct operations. Access may be controlled on military installations to enhance OPSEC. The PA office advises the commander

on the information demands anticipated, information strategies available, and the overall communications effort. Regardless of how military units provide PA support, commanders should always involve their PA personnel when planning HD operations. Public affairs activities can be employed to gain and maintain public support for military operations and communicate US resolve.

*For further details, see JP 3-61, Doctrine for Public Affairs in Joint Operations.*

d. **Rules of Engagement (ROE) and Rules for the Use of Force (RUF).** The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3121.01, *Standing Rules of Engagement for US Forces*, and DODD 5210.56, *Use of Deadly Force and the Carrying of Firearms by DOD Personnel Engaged in Law Enforcement and Security Duties*, establishes fundamental policies and procedures governing the actions to be taken by US commanders during military HD operations. Supplemental ROE may be required for a period of time depending on the situation and the mission area the DOD is tasked to perform.

## CHAPTER IV CIVIL SUPPORT

*“The Secretary of Defense shall provide military support to civil authorities for domestic incidents as directed by the President or when consistent with military readiness and appropriate under the circumstances and the law. The Secretary of Defense shall retain command of military forces providing civil support. The Secretary of Defense and the Secretary [of Homeland Security] shall establish appropriate relationships and mechanisms for cooperation and coordination between their two departments.”*

**Homeland Security Presidential Directive-5  
28 February 2003**

### 1. General

a. **DOD shall cooperate with and provide support to civil authorities as directed by and consistent with laws, Presidential directives, EOs, and DOD policies and directives.** Military commanders ensure that DOD resources are used judiciously by adhering to the following principles:

(1) DOD resources are provided only when response or recovery requirements are beyond the capabilities of local, state, and federal civil authorities, and when they are requested by an LFA and approved by SecDef. An exception to this is in the case of immediate response authority (see DODD 3025.1, *Military Support to Civil Authorities*) when local commanders can respond to save lives, prevent human suffering, or mitigate great property damage,

(2) DOD specialized capabilities (e.g., airlift and reconnaissance) are used efficiently.

(3) SecDef shall retain control of assigned Title 10 military forces providing CS. The dual federal-state mission of the NG, organized under the supervision of the adjutant general and the direction of the governor in each state/territory, makes it likely that the NG will be the first military responder during a CS event. This early employment of NG will be in a state active duty or Title 32 status under the direction of the governor, and generally well in advance of a formal federal response request being generated. There are advantages associated with employment of the NG in either state active duty (under state control and state funded) or Title 32 status (under state control but federally funded, usually for training or limited operations), most notably no Posse Comitatus constraints. Also, most, if not all, deployed NG forces will remain in Title 32 status throughout an event. **Therefore, a combined response made up of Title 10, 14, 32, and /or state active duty forces may be employed in response to individual incidents or events.**

Note: There are special circumstances when the President and the governor of an affected state both authorize a state National Guard commander to be placed on Title 10 status and retain Title 32 authority. In this case Title 10 forces may be placed under the control of this commander who reports to both the governor (for state requirements) and the supported combatant commander (for DOD mission assignments) through an interplay of 32 USC 315 and 325 and 10 USC 104.

(4) DOD components do not perform any function of civil government unless authorized.



*The most visible type of assistance DOD provides is support to civil authorities for domestic emergencies or disasters.*

b. **The US military organizes, trains, and equips forces primarily to conduct combat operations.** Inherent within the combat capabilities of the Services, is the military's ability to rapidly respond to assist civil authorities for domestic emergencies such as disasters, authorized law enforcement, and other activities that exceed the capability of civilian agencies. This capability described as CS is one of two HS mission areas for DOD.

c. **The most visible type of assistance DOD provides is support to civil authorities for domestic emergencies or disasters.** DOD responds to such incidents in accordance with federal policies, DODDs, and individual agreements. The complexity of such incidents requires extensive interagency coordination and follows a specific request process.

d. DOD provides support to a variety of interagency organizations, including LEAs, in accordance with US laws and DOD directives. Agreements between DOD and other interagency organizations may help in defining the scope of support to be provided either routinely or in an emergency. However, these agreements do not pre-approve support. SecDef will approve all support of civil authorities. Actions taken under immediate response authority are the only exception; however, commanders must report and gain approval from the Secretary through the NMCC at the earliest possible opportunity.

## **2. Civil Support Characteristics**

a. **DOD's planning considerations are key to developing a viable CS strategy.** DOD plays a key role in CS and supports several response plans as well as agreements with other agencies.

Because DOD has the statutory mission to defend the Nation from attack, SecDef retains the authority to disapprove any requests for CS from the interagency if the requests distract from this primary mission, unless otherwise directed by the President. The combatant commanders responsible for HD and CS (CDRUSNORTHCOM and CDRUSPACOM) incorporate plans for CS by task organizing their commands to accomplish CS missions as well as other assigned missions. DOD is a signatory to numerous response plans as well as various memoranda of understanding (MOUs) and MOAs with other agencies; therefore, DOD plays a critical role in CS and is relied on by many agencies.

**b. The preparedness of DOD’s assets is critical to accomplishing its worldwide military operations as well as to any CS mission to which it responds.** DOD frequently participates in interagency working groups and exercises. The capabilities of DOD, particularly in specialized assets such as explosive ordnance disposal (EOD) teams, technical escort units, the Chemical and Biological Incident Response Force, and JTF-CS, lend a capacity to civilian agencies that may not have the means to manage a CBRNE event. By exercising with civil authorities, DOD’s CM capabilities are not only enhanced; it allows the civil authorities to appreciate what DOD can provide in a crisis.

**c. The response measures taken by DOD are in accordance with its capabilities, current laws, PDDs, EOs, and DOD policies, directives, and orders.** When DOD considers the measure of its response to a request for assistance (RFA) by a civilian authority, it must take into consideration previous planning that has been done on the scenario as well as the overall preparedness of the assets DOD plans to use. The Office of the Secretary of Defense must also validate RFAs using specific criteria that are discussed later in this chapter.

**d. In certain circumstances, imminently serious conditions resulting from either civil emergencies or attacks may require immediate response by military commanders, or by responsible officials of other DOD agencies.** Responses to requests from civil authorities prior to receiving authority from the President or chain of command are made when immediate support is critical to save lives, prevent human suffering, or mitigate great property damage. When such conditions exist and time does not permit prior approval from higher headquarters, commanders or officials acting under immediate response authority may take necessary action to respond, but must advise the NMCC through command channels by the most expeditious means available and seek approval or additional authorizations. The military will begin disengagement from immediate response activity as soon as practicable. While immediate response should be provided to civil agencies on a cost-reimbursable basis if possible, it should not be delayed or denied because of the inability or unwillingness of the requester to make a commitment to reimburse the Department of Defense.

*For more information on immediate response authority see DODD 3025.15, Military Assistance to Civil Authorities, and DODD 3025.1, Military Support to Civil Authorities.*

**e. Unless prior agreements or arrangements are in place and outside of the conditions cited for “immediate response” DOD usually provides support only in response to a validated RFA.**

### 3. Civil Support Mission Area

**Employment of military forces within the US, its territories, and possessions, under the auspices of CS, typically falls under the broad mission of MACA.** MACA missions, for the purposes of this publication, consist of three mission subsets (see Figure IV-1). These mission subsets are MSCA, MSCLEA, and MACDIS.

a. **Military Support to Civil Authorities.** MSCA is the most widely recognized form of DOD CS because it usually consists of support for high-profile emergencies such as natural or manmade disasters that often invoke Presidential or state emergency/disaster declarations (see Figure IV-2). DOD assistance should be requested by an LFA only when other local, state and federal capabilities have been exhausted or when a military-unique capability is required.

(1) **Natural Disasters.** In the event of a natural disaster or emergency, there will be a concerted US Government effort to support the affected areas. As a signatory to the NRP, DOD may be asked to provide assistance to DHS/FEMA in an attempt to save lives, protect property and lessen the threat of a catastrophe in the US. Examples of natural disasters include, but are not limited to severe weather, wildfires, and outbreaks of animal disease. When natural disasters occur and military assistance is anticipated, DHS/FEMA will request a defense coordinating officer (DCO) who serves as the single DOD point of contact within the disaster area. The DCO will be OPCON to the designated supported combatant commander or designated JTF commander. Certain capabilities with a global focus, such as airlift and space assets, will normally be provided in support rather than the SecDef authorizing a change in OPCON.

(2) **Special Events.** DOD is often asked to provide support to a special event, a planned program of athletic competition or related activities involving participants from the US and/or other nations. Historic examples of these events are the Olympic Games and the Pan American Games.



Figure IV-1. Civil Support Missions



Figure IV-2. Military Support to Civil Authorities

SecDef may also designate non-athletic international or national events to receive support in accordance with DODD 2000.15, *Support to Special Events*. Other examples of non-athletic events include summits, world fairs, and the Boy Scout Jamboree. The LFA for special events can vary. Special events may differ from an NSSE and are identified as special events for homeland security (SEHS), Levels 1 through 4. Within the interagency arena, SEHS events are of lesser National importance or significance than NSSEs, but still qualify for some level of Federal support and/or monitoring. SEHS Level 1 events are more important than SEHS level 4 events and would qualify for more Federal assistance and support. An NSSE is a specific designation given by the Secretary of Homeland Security and are led by USSS.

(3) **Manmade Disasters.** Manmade disasters can be accidental or intentional. An example of an accidental event is an oil spill. CBRNE-CM could be initiated in response to an accident or an intentional terrorist act. The implications of a deliberate or unintentional large release of a CBRNE are severe. A catastrophic CBRNE event or attack may occur with little or no warning, resulting (either immediately or over time) in mass casualties and producing a mass exodus of evacuees. The response capabilities and resources of the local jurisdiction (to include mutual aid from surrounding jurisdictions and response support from the state) may be insufficient and quickly, if not immediately, overwhelmed. As a result, the nature and scope of such a catastrophic event or attack will initiate an immediate federal response. Therefore, specific attention has been focused on task-organizing within DOD to plan for and integrate its support to an LFA to manage the consequences of a domestic CBRNE event.

b. **Military Support to Civilian Law Enforcement Agencies.** The use of the military in law enforcement roles is a sensitive topic and restrictions apply to such use. Military forces performing in this role may work under several LFAs to include DHS or DOJ/FBI, and may be armed depending on the circumstances. SecDef will decide whether or not units will be armed. Military support to civilian LEAs may include, but is not limited to NSSEs, support for combating terrorism, support to CD operations, maritime security, ISR capabilities, and general support (training support to law enforcement agencies/loan of equipment/personnel and expert advice).



(1) **Counterterrorism (CT) Support.** Acting through the FBI, the Attorney General, in cooperation with the heads of other Federal departments, agencies, and military criminal investigative organizations, coordinates domestic intelligence collection and the activities of the law enforcement community to detect, prevent, preempt, and disrupt terrorist attacks, and to identify the perpetrators and bring them to justice in the event of a terrorist incident. DOD may be requested to support the FBI or other LEAs during the CrM portion of a response. If there is a credible threat, DOD may also be requested to support LEAs in a pre-positioning of forces. Under this type of support, specific RUF must be established and approved. In the absence of preexisting RUF, such as are contained in DODD 5210.56, *Use of Deadly Force and the Carrying of Firearms by DOD Personnel Engaged in Law Enforcement and Security Duties*, requests for RUF for CS missions will be sent through the supported combatant commander to DOD for development and approval. Supplemental RUF may be required depending on the situation.

*For more information on CT see JP 3-07.2, Joint Tactics, Techniques, and Procedures for Antiterrorism.*

(2) **National Special Security Event Support.** NSSEs are events of national significance that require greater federal visibility. NSSE is a designation that was established by PDD 62 and HSPD-7 (which supersedes the language in the PDD) and provides for additional federal resources in support of state and local authorities. If DOD assistance is required, military forces will remain in a supporting role to the LFA. The Secretary of Homeland Security, in consultation with the HSC, shall be responsible for designating events as NSSEs. The USSS, an element of the DHS, is the LFA for NSSE-designated events. Special events, including NSSEs, are ranked in importance by the FBI.



*Historic examples of National Special Security Events include the Olympic Games.*

Historical examples of NSSEs include the State of the Union Address, Salt Lake City Olympics, and Democratic and Republican National Conventions.

(3) **Counterdrug Operations Support.** The US approach to CD has evolved into a comprehensive program of actions employing a multinational and multi-agency approach to the problem of illegal drugs. CD planning involves joint, multinational, and interagency organizations and requires close coordination. In performance of CD operations DOD will be in support of another LFA. DEA serves as the lead LEA for coordinating domestic CD LEA efforts. DOD's principal CD mission is the detection and monitoring of the transit of illegal drugs into the US.

*For more information on CD see JP 3-07.4, Joint Counterdrug Operations.*

(4) **Maritime Security.** The USCG, when operating under DHS, is responsible for the conduct and coordination of maritime HS operations. When the USCG is serving in this role, DOD support may be requested. Potential DOD support may include the provision of ships to assist with boarding operations during heightened maritime security levels; aircraft for merchant ship surveillance; EOD teams for port security; or mine clearance operations. When supporting maritime law enforcement activities, US Navy ships will require the embarkation of USCG law enforcement detachments.

(5) **Loans of Equipment, Facilities, or Personnel to Law Enforcement.** Requests for loans of equipment, facilities, or personnel made by LEAs, including the USCG when not acting as part of the Navy, shall be made and approved in accordance with DODD 5525.5, *DOD Cooperation with Civilian Law Enforcement Officials*, but at a level no lower than a flag or general officer, or equivalent civilian, except for requests for potential lethal support. **SecDef is the approval authority for any requests for potentially lethal support** (i.e., lethal to the public, a member of law enforcement, or a Service member) made by LEAs.

c. **Military Assistance for Civil Disturbances.** The President is authorized by the Constitution and statutory laws to employ the Armed Forces of the United States to suppress insurrections, rebellions, and riots, and provide federal supplemental assistance to the states to maintain law and order (see Figure IV-3). Responsibility for the management of federal response for civil disturbances rests with the Attorney General. **However, any DOD forces employed in MACDIS operations shall remain under military C2 at all times.**

#### 4. Supporting Operations and Enabling Activities

**When performing missions associated with CS, DOD will always serve in a supporting role.** The following, although not an inclusive list, describes supporting operations and enabling activities commonly associated with CS missions.

a. **Incident Management.** HSPD-5 states that the US Government shall establish a single, comprehensive approach to domestic incident management that treats CrM and CM as a single integrated function. Incident management includes measures and activities performed at the national level and includes crisis and consequence management activities. **The overarching policy of incident management can be thought of in two overlapping phases, crisis and consequence management.**

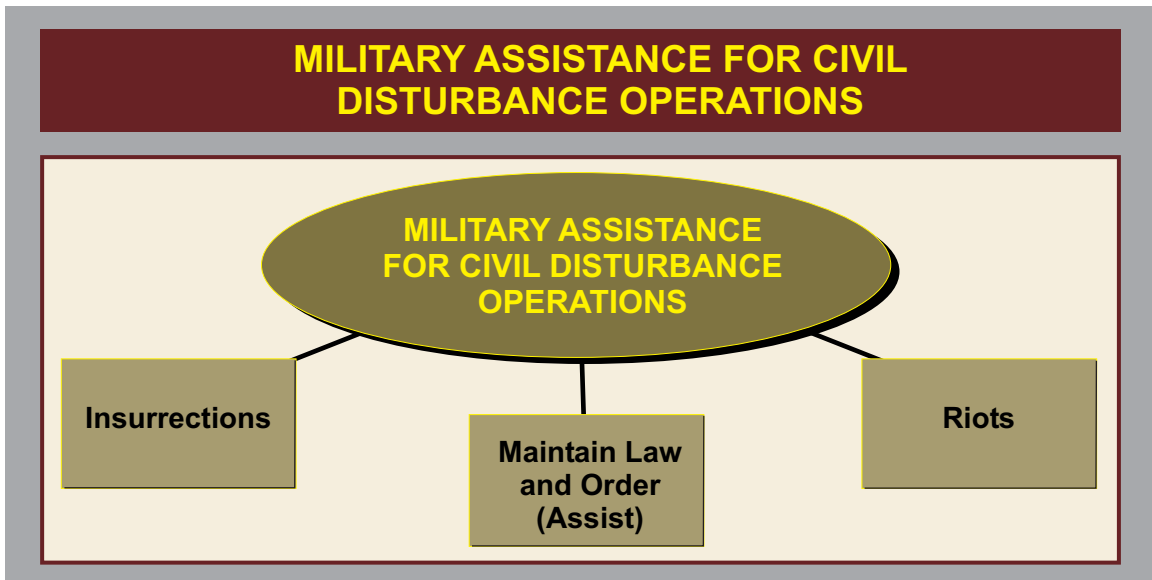


Figure IV-3. Military Assistance for Civil Disturbance Operations

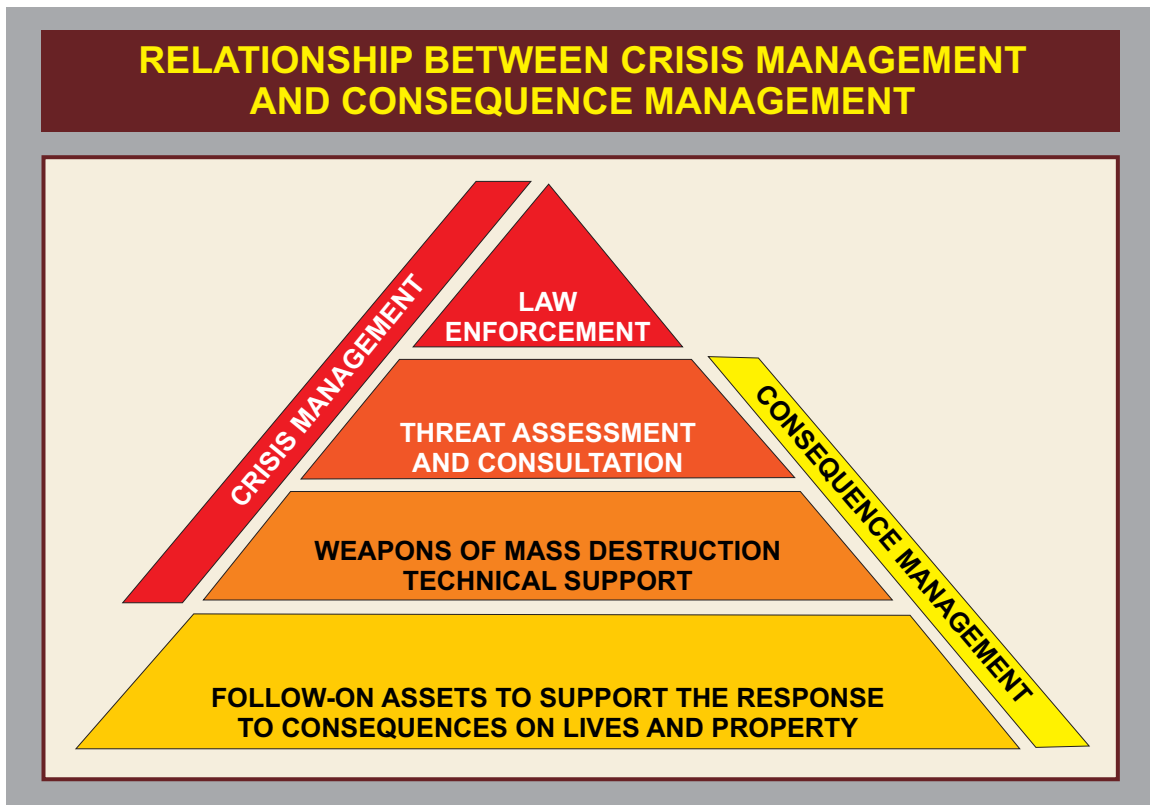
#### NATIONAL INCIDENT MANAGEMENT SYSTEM

**“Incident: An occurrence or event, natural or human-caused, that requires an emergency response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, wildland and urban fires, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response”**

**SOURCE: March 1 2004, Department of Homeland Security**

(1) **Crisis Management.** CrM refers to measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or an act of terrorism. PDD-39, *US Policy on Counterterrorism*, designates DOJ, specifically the FBI, as the LFA for CrM. The Federal government exercises primary authority to prevent, preempt, and terminate threats or acts of terrorism and to apprehend and prosecute the perpetrators, and state and local governments provide assistance as required. CrM is predominantly a law enforcement response and in such cases involves measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism under federal law. See Figure IV-4 for a depiction of the relationship between CrM and CM.

(2) **Consequence Management.** CM includes those actions required to manage and mitigate problems resulting from disasters and catastrophes. It may include COOP/COG measures to restore essential government services, protect public health and safety, and provide emergency relief to affected governments, businesses, and individuals. Responses occur under the primary jurisdiction of the affected state and local government, and the Federal government provides assistance when required. When situations are beyond the capability of the state, the governor requests federal assistance

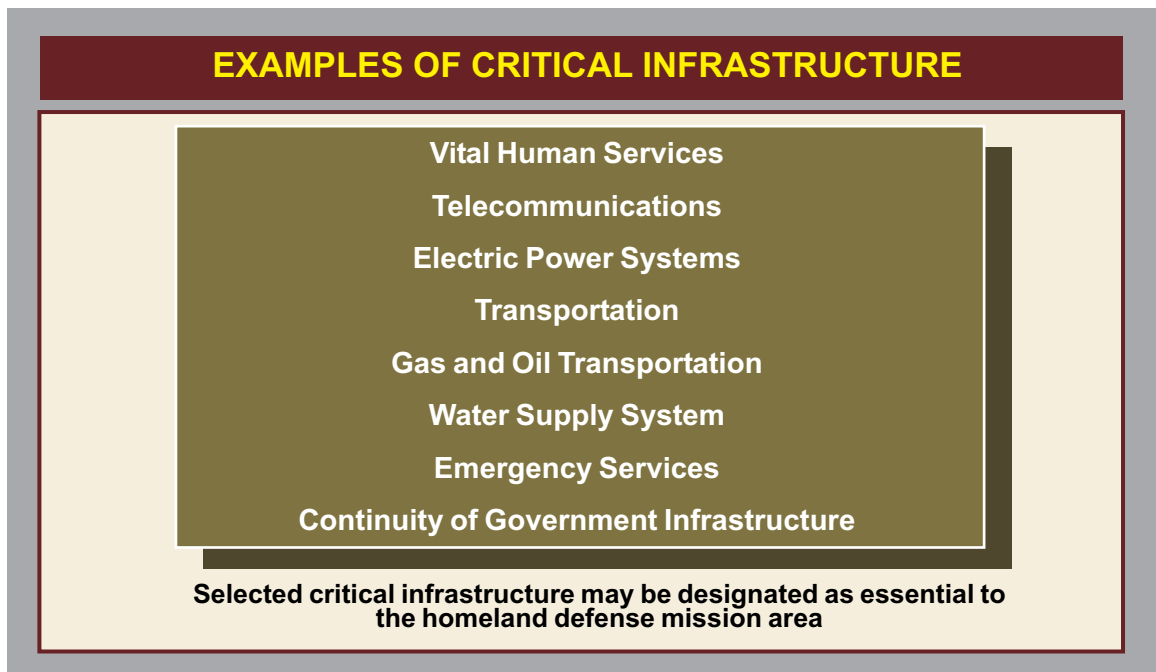


**Figure IV-4. Relationship Between Crisis Management and Consequence Management**

through the President. The President may also direct the Federal government to provide supplemental assistance to state and local governments to alleviate the suffering and damage resulting from disasters or emergencies. DHS/FEMA has the primary responsibility for coordination of federal CM assistance to state and local governments.

b. **Technical Operations.** Based on the situation, a federal CrM response may be supported by technical operations and by federal CM, which may operate concurrently. Technical operations include actions to identify, assess, dismantle, transfer, dispose of, or decontaminate personnel and property exposed in a CBRNE incident. The LFA for technical operations depends upon the material involved and the location of the incident. Other federal agencies supporting technical operations include DOE, DHHS, and the EPA.

c. **Critical Infrastructure Protection.** While DOD is responsible for DCI, there may be instances where the President and SecDef will instruct DOD to provide support to other LFAs. This support can take many forms but is normally associated with disasters, emergency relief, CrM and CM activities. **Critical infrastructure comprises those systems essential to the minimum operations of the economy and the government.** They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private (see Figure IV-5). Many of the nation's critical infrastructures have historically been separate systems that had little interdependence. However, as a result of advances in information technology and the necessity to improve efficiency, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities (e.g., equipment failures, human error, weather and other natural causes, as well as, actual attack). Addressing these vulnerabilities will



**Figure IV-5. Examples of Critical Infrastructure**

require new and flexible approaches spanning the public and private sectors to protect domestic and international security. **The United States' economy is also increasingly reliant upon interdependent and network-supported infrastructures.** Nontraditional attacks on these infrastructures and other information systems may be capable of significantly harming the national economy and our ability to project military power. Adversaries, whether nations, groups or individuals, will likely attempt to employ asymmetric attacks to impair or destroy critical infrastructure by avoiding our strengths and exploiting our actual or perceived weaknesses.

## **5. Department of Defense Civil Support Process**

a. **Functionality.** In January 2003, pursuant to the National Defense Authorization Act of Fiscal Year 2003, SecDef established the ASD(HD). In addition to overseeing HD activities, SecDef vested the roles and responsibilities associated with the DOD Executive Agent for MSCA and MACDIS with ASD(HD).

### **b. Command, Control, and Coordination**

(1) In March 2003, the roles and responsibilities associated with the DOD Executive Agent for MSCA and MACDIS were rescinded. **ASD(HD) was subsequently assigned the responsibility for the support within DOD.** SecDef also transferred the functions and associated resources of the Army's Office of the Director of Military Support to the Joint Chiefs of Staff office of the Joint Director of Military Support (JDOMS). Guidance from SecDef or the ASD(HD) is translated into operational orders developed by JDOMS. JDOMS produces military orders as they pertain to domestic emergencies, forwards them to SecDef for approval and then to the appropriate military commander for execution. Figure IV-6 depicts specific functions and tasks the ASD(HD) and JDOMS will perform in the event DOD receives

a RFA. CDRUSNORTHCOM and CDRUSPACOM are the supported combatant commanders within their AORs for mission execution. **Only the Secretary of Defense can authorize the deployment of forces for MACA missions.** Specific command and control arrangements for CS operations are addressed in Chapter II, “Command Relationships and Interagency Responsibilities.” Figure IV-6 represents a typical RFA, however, there may be exceptions to this procedure.

(2) DOD support to a CBRNE CM situation is similar to DOD support for routine MSCA operations. Upon a validated request from the LFA to the executive secretary (EXECSEC), DOD will provide assistance. (The EXECSEC is part of the Immediate Office of the Secretary of Defense and is the head of an organization known as the Executive Secretariat. The EXECSEC provides direct administrative support to the Secretary and Deputy Secretary of Defense.) CDRUSNORTHCOM and CDRUSPACOM will serve as the supported commanders within their AORs for CBRNE CM activities. For large CBRNE CM events within CONUS, USNORTHCOM may deploy JTF-CS, which will exercise OPCON over designated DOD forces. The DCO is the DOD single point of contact in the joint field office for requests for DOD assistance. Any requests for DOD assistance should be processed in accordance with the NRP.

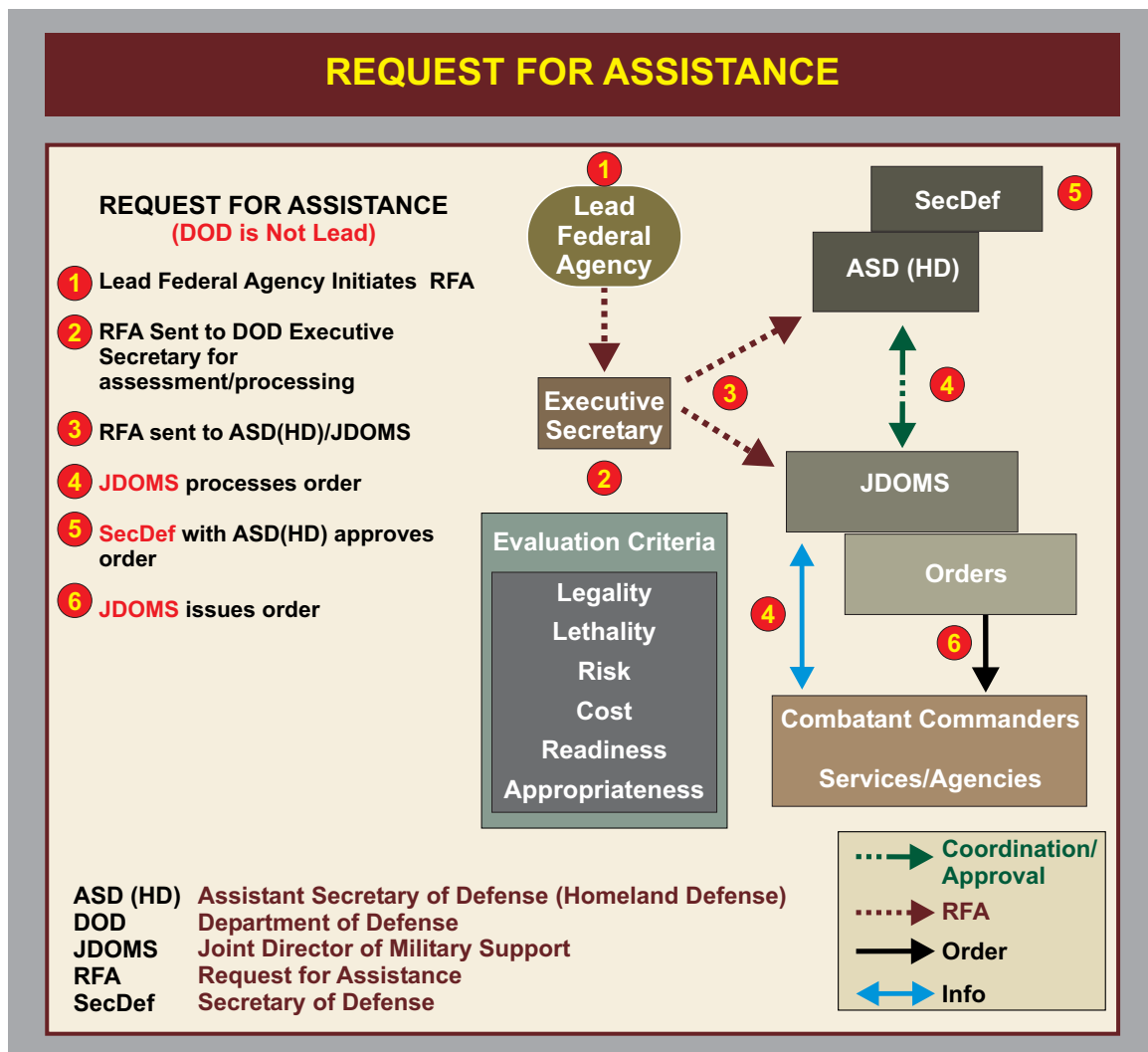


Figure IV-6. Request for Assistance

(3) While executing CS missions, DOD personnel work closely with civilian officials from federal, state, and local governments, as well as volunteer and nongovernmental agencies. The need to coordinate activities in nonmilitary terms is of the utmost importance. This requires an understanding of the terms and needs of the other agencies.

*See JP 3-08, Interagency Coordination During Joint Operations, for additional information.*

c. **Requests for Assistance.** As previously outlined, DOD is always in a supporting role when performing in the CS mission area. In accordance with the NRP, DOD may provide equipment or assets when the mission does not interfere with its military functions. The type and extent of requests for DOD assistance are wide-ranging and in order to expedite DOD support, RFAs must be submitted through the EXECSEC, who will forward them to ASD(HD) for validation. Since CS is not DOD's primary mission, all requests for DOD military assistance are evaluated against the following criteria: legality, readiness, lethality, risk, cost, and appropriateness. Given that CS missions involve life-saving responses, this process is rapidly executed to expedite the prompt movement of forces and support. **Except in cases of immediate response, DOD cannot provide MACA without an official request from another federal agency or direction from the President.** If a disaster is of such proportions to generate mass casualties in need of evacuation, DOD acts as the lead for this function under the National Disaster Medical System. However, the majority of CS provided by DOD on a regular basis is typically some form of MSCLEA.

d. **Mechanisms.** All military assistance must be requested in some fashion.

(1) **MOA/MOU.** Agreement between DOD and other interagency organizations may help in defining the scope of support to be provided; either routinely or in an emergency. However, these agreements do not pre-approve support. All requests will be submitted to the DOD EXECSEC and SecDef will approve all support of civil authorities. Actions taken under immediate response authority are the only exception; however, commanders must report and gain approval from the Secretary through the DOD EXECSEC at the earliest possible opportunity.

(2) **Federal Emergency Plans and Contingency Plans.** CS is a concerted national program that utilizes local, state, tribal, and federal assets. There is a family of emergency response and contingency plans that defines the roles, responsibilities, and funding mechanisms for various incident management circumstances.

(a) **National Response Plan.** The most prominent CS plan is the **NRP, which is the primary Federal mechanism through which DOD support is requested for domestic emergencies.** The NRP describes the policies, planning assumptions, and a concept of operations that guide federal operations following a Presidential declaration of a major disaster or emergency. The NRP is coordinated and managed by DHS/FEMA and is the result of agreements between DHS/FEMA and the primary and supporting federal agencies responsible for providing disaster relief support. The primary agency for resource support under the NRP is the GSA. Supporting agencies include the following Departments: Agriculture, Commerce, Defense, Energy, Labor, Transportation, Treasury, and Veterans Affairs. The following agencies also have major roles in the execution of the NRP: DHS/

FEMA, National Aeronautics and Space Administration, National Communications System, and the Office of Personnel Management. DOD resource support under the NRP includes personnel, equipment, and supplies in the absence of other national disaster system resource capabilities. Support is provided with the provision that it does not conflict with DOD's mission or its ability to respond to operational contingencies.

(b) **National Response Plan.** HSPD-5 directed the Secretary of Homeland Security to develop and administer an NRP to integrate the current family of federal domestic prevention, preparedness, response and recovery plans into a single all-discipline, all-hazards plan in an attempt to unify domestic incident management. The NRP has superseded other emergency response plans (e.g., US Government Interagency Domestic Terrorism Concept of Operations Plan, Federal Radiological Emergency Response Plan, Mass Migration Emergency Plan, and the National Oil and Hazardous Substances Pollution Contingency Plan). In addition to consolidating federal plans, other modifications within the NRP that impact DOD are the establishment of a Homeland Security Operations Center, the establishment of an interagency incident management group, and the creation of a principal federal official who may be appointed to represent the Secretary of Homeland Security at the incident site. Details of the NRP will be addressed in JP 3-26.2, *Joint Doctrine for Civil Support*.

e. **National Incident Management System.** The system will provide all of the Nation's first-responders and authorities with the same foundation for incident management in terrorist attacks, natural disasters, and other emergencies. Key elements and features of NIMS include: an Incident Command System, a Joint Information System, and an NIMS Integration Center.

## 6. Planning Considerations for Civil Support Operations

a. **Operational Stages.** The NRP identifies a spectrum of activities for incident management (e.g., prevention, preparation, response, and recovery). **CS operations will normally be conducted during the response stage of domestic incident management.** Response operations focus on those lifesaving and sustaining functions required by the population in the disaster area. Recovery operations begin the process of returning the community infrastructure and services (both municipal and commercial) to a status that satisfies the needs of the population. Military forces normally redeploy as operations transition from the response to the recovery stage. Transition planning is based on completion of those CS tasks being accomplished by DOD forces, or unfinished mission assignments being transferred back to civil agencies at the federal or state level. This practice allows the military to return to its defense roles as soon as practicable.

b. **Simultaneous Operations.** CS may take place simultaneously with other military operations during national security emergencies. Consequently, there may be competing requirements for units and support such as transportation, equipment, and supplies that must be balanced with commitments elsewhere in the world. Asset-sourcing conflicts must be quickly resolved to prevent delays in responding to time-sensitive requirements.

c. **Legal Considerations.** The authorities governing the employment of US military forces in CS operations consist of federal laws, executive directives, DOD plans and policies, and other directives, instructions, and regulations, making a comprehensive legal reviews of CS plans essential.



(1) Sound legal advice during MACA operations will ensure that the application of military capabilities and resources is within the constraints of the law. Commanders involved in CS shall staff plans, policies, programs, exercises, funding, operations, constraints, and limitations with their judge advocates (JAs) to ensure conformity with legal requirements. Federal, state, and local governments execute US laws with the assistance of LEAs. The Domestic Operational Law Handbook for Judge Advocates, from the Center for Law and Military Operations, provides specific legal guidance for DOD CS. JAs should have access to this publication.

(2) Limited military support to LEAs is allowed under laws such as 10 USC Sections 371-381. Under these laws, the military may share certain information and provide equipment, facilities, and other services to LEAs. The Fiscal Year 1991 National Defense Authorization Act allows certain types of military support for the national CD effort. The authority and funding for these activities have been extended in subsequent authorization acts so that they are still current, and may be extended again. DOD policies for providing military support to LEAs, including personnel and equipment, are contained in DODD 5525.5, *DOD Cooperation with Civilian Law Enforcement Officials*.

*For more information on authorities see Appendix A, “Key Homeland Security Legal and Policy Documents.”*

d. **Rules for the Use of Force.** Depending on the type of CS mission, different RUF apply:

(1) **MSCA. The standing rules of engagement as delineated in CJCSI 3121.01A, *Standing Rules of Engagement for US Forces*, do not apply to US forces conducting MSCA missions.** US forces deployed to assist federal and local authorities in disaster assistance missions, such as hurricanes and earthquakes, follow RUF as set forth in the mission’s execute order and subsequent orders. In support of CBRNE CM operations, RUF are delineated in CJCS CONPLAN 0500, Annex C, Appendix 16, *Rules for the Use of Force*. There is a presumption that units deployed to sites of a CBRNE situation will not carry arms. As authorized by SecDef, units may deploy to sites with their weapons stored in an appropriate storage container to cover possible follow-on assignments where weapons are authorized. Military commanders are responsible to ensure that weapons and ammunition are properly stored and physically secured at any incident response site.

(2) **MSCLEA.** Forces deployed to assist LEAs may or may not be armed depending on the situation. These forces will adhere to the RUF as designated in the deployment order or MOA with the supported federal LEA. Forces conducting CD missions abide by RUF in CJCSI 3121.02, *Rules on the Use of Force by DOD Personnel Providing Support to Law Enforcement Agencies Conducting Counterdrug Operations in the United States*.

(3) **MACDIS.** Forces deployed to assist federal and local authorities during times of civil disturbance situations follow the use-of-force policy found in *DOD Civil Disturbance Plan—GARDEN PLOT* (Appendix 1 to Annex C) and Director of Military Support message 161639Z July 1996, Subject: *Changes to DOD Civil Disturbance Plan*.

(4) **In CS, appropriate military capabilities are applied prudently and with restraint.** RUF are restrictive, detailed, and sensitive to political concerns and may change frequently during operations. Restraints on weaponry, tactics, and levels of force characterize this mission area.

(5) Commanders should consult their JAs regarding the implementation of any training program on RUF. RUF should be continually stressed during the operation. Written guidance, frequent information update briefings, and brief-backs are methods to ensure that military forces understand procedures.

e. **Funding.** Authorities and funding are main issues that impact DOD's ability to respond. Cost reimbursement for CS is usually in accordance with the Economy Act, Title 31, USC Sec 1515, which mandates cost reimbursement by the federal agency requesting support. However, when a Presidential Disaster or Emergency Declaration is declared, the Stafford Act sets the guidelines for reimbursements to federal agencies and states from federal funds set aside to support these missions.

*See JP 1-06, Joint Tactics, Techniques, and Procedures for Financial Management During Joint Operations, for more information.*

f. **Concurrent Assistance to Civilian Agencies. Military responses to a credible threat and acts of terrorism may require both CrM and CM operations.** These operations may often overlap. DOJ/FBI is the overall LFA in preventing or resolving threats involving terrorism and for crisis response throughout a terrorist threat or act. DHS/FEMA leads CM operations and is the LFA for emergency response actions to lessen or mitigate the consequences of attacks or incidents. In some situations, CM may include pre-event planning for one incident while conducting post-event operations for another. DOD direct support for CM is provided to DHS/FEMA or an NRP primary agency. Under these circumstances, supporting elements should coordinate, integrate, and synchronize their activities and operations.

g. **Public Affairs.** CS usually draws extensive media attention. **Military PA activities are subject to approval of the LFA.** Military public affairs officers (PAOs) operate in an interagency environment, with emphasis on cooperation, coordination, and unity of effort. Access for the media is normally regulated to ensure OPSEC; however the public's impression of the assistance depends to a great extent on the media. This perception also influences the cooperation and coordination between commanders and civilian leaders. Positive public support facilitates mission accomplishment. Lack of public support, on the other hand, can seriously impede the effectiveness of military forces during the execution of CS missions. Complete integration of PA personnel in all staff planning is essential to ensure an effective PA operation. News media access to CS operational areas is subject to the approval of the LFA. PAOs operate under the conditions imposed by the government agency that has jurisdiction. The LFA has release authority. The military must coordinate all PA activities with the LFA and comply with its PA guidance.

*See JP 3-61, Doctrine for Public Affairs in Joint Operations, for additional information.*

h. **Chaplain.** Military chaplains may deploy in response to CM events. Requests will be from the LFA through the federal coordinating officer, the DCO, and/or the on-scene JTF commander. Accordingly, military chaplains may provide religious support to civilian disaster victims during emergency operations.

This ministry will be limited to the designated disaster control area and will cease with the termination of emergency operations. Moreover, the primary focus of military chaplain ministry will remain DOD personnel.

*See JP 1-05, Religious Support for Joint Operations, for more information.*

i. **Environmental Considerations.** Commanders should make environmental considerations an integral part of the mission planning and operational decision-making process. All joint operations within the US and US territories shall be conducted in compliance with applicable federal, state, and local environmental regulatory guidance. Adverse environmental impacts should be avoided or mitigated when practicable, based on mission requirements and response to emergency situations.

*For further information, see JP 3-34, Joint Doctrine for Engineering Support, and JP 4-04, Joint Doctrine for Civil Engineering Support.*

## APPENDIX A

### KEY HOMELAND SECURITY LEGAL AND POLICY DOCUMENTS

#### 1. Legal and National Policy and Guidance

There are a variety of documents that provide guidance for the HS mission areas. These range from the US Constitution to the Contingency Planning Guidance.

a. **The Constitution.** The Preamble states that two of the purposes of the Constitution are to insure domestic tranquility and provide for the common defense. Furthermore, Congress has the power to declare war, raise and support armies, provide and maintain a Navy, and provide for calling forth the militia to execute the laws of the Union, suppress insurrections and repel invasions. The President is the Commander in Chief of the Armed Forces. The Constitution provides the fundamental justification for HS through the guarantee of domestic tranquility and provision for the common defense of the nation.

b. **Key Executive and Legislative Guidance.** The following documents are key references when addressing HS mission areas:

(1) **Homeland Security Presidential Directive/HSPD-1.** *Organization and Operation of the Homeland Security Council* (October 29, 2001) established the HSC to ensure coordination of all HS-related activities among the executive departments and agencies and promote the effective development and implementation of all HS policies.

(2) **Homeland Security Presidential Directive/HSPD-2.** *Combating Terrorism Through Immigration Policies* (29 October 2001). HSPD-2 established policies and procedures to prevent aliens who engage in or support terrorist activity from entering the US and to detain, prosecute, or deport any such aliens who are within the US.

(3) **Homeland Security Presidential Directive/HSPD-3.** *The Homeland Security Advisory System* (11 March 2002). HSPD-3 provides the guidelines for a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to federal, state and local authorities and the American people. This document establishes the five threat conditions and their respective protective measures.

(4) **Homeland Security Presidential Directive/HSPD-4.** *National Strategy to Combat Weapons of Mass Destruction* (December 2002). HSPD-4 describes three pillars for our national strategy to combat WMD: counterproliferation to combat WMD use, strengthen nonproliferation to combat WMD proliferation, and consequence management to respond to WMD use. Each pillar iterates specific actions to be pursued within the pillar.

(5) **Homeland Security Presidential Directive/HSPD-5.** *Management of Domestic Incidents* (28 February 2003). Assigns the Secretary of the Department of Homeland Security as the principal Federal official for domestic incident management to coordinate the Federal Government's resources utilized in response to, or recovery from terrorist attacks, major disasters,

or other emergencies. The Federal Government assists state and local authorities when their resources are overwhelmed, or when Federal interests are involved. Nothing in the directive impairs or otherwise affects the authority of SecDef over DOD, including the chain of command for military forces. SecDef provides military support to civil authorities for domestic incidents as directed by the President. SecDef retains command of military forces providing civil support. Additionally, HSPD-5 established NIMS to provide a consistent nationwide approach for Federal, state, and local governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents. It directs the development of the NRP and includes classified annexes if required. The NRP, using NIMS, with regard to response to domestic incidents, provides the structure and mechanisms for national level policy and operational direction for Federal support to state and local incident managers.

(6) **Homeland Security Presidential Directive/HSPD-6.** *Integration and Use of Screening Information* (16 September 2003). HSPD-6 provides for the development and maintenance of accurate and current information about individuals known or appropriately suspected to be or have been engaged in conduct related to terrorism; and that information, as appropriate and permitted by law, can be used to support screening and protective processes via the Terrorist Screening Center.

(7) **Homeland Security Presidential Directive/HSPD-7.** *Critical Infrastructure Identification, Prioritization, and Protection* (17 December 2003). HSPD-7 established a national policy for federal departments and agencies to identify and prioritize US critical infrastructure and key resources and to protect them from terrorist attacks. This directive identifies roles and responsibilities of the Secretary of Homeland Security, and other departments and recognizes DOD as the sector-specific agency for the Defense Industrial Base.

(8) **Homeland Security Presidential Directive/HSPD-8.** *National Preparedness* (17 December 2003). HSPD-8 established policies to strengthen the preparedness of the United States to prevent and respond to threats and actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of federal preparedness assistance to state and local governments, and outlining actions to strengthen preparedness capabilities of federal, state, and local entities.

(9) **Homeland Security Presidential Directive/HSPD-9.** *Defense of United States Agriculture and Food* (30 January 2004). HSPD-9 established a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies.

(10) **Homeland Security Presidential Directive/HSPD-10.** *Biodefense for the 21st Century* (28 April 2004). HSPD-10 provides a comprehensive framework for the Nations's biodefense and, among other things, delineates the roles and responsibilities of Federal agencies and departments in continuing their important work in this area.

(11) **Homeland Security Presidential Directive/HSPD-11.** *Comprehensive Terrorist-Related Screening Procedures* (27 August 2004). HSPD-11 establishes procedures to enhance terrorist-related screening through comprehensive, coordinated procedures that detect, identify, track,

and interdict people, cargo, conveyances, and other entities and objects that pose a threat to homeland security.

(12) **Homeland Security Presidential Directive/HSPD-12.** *Policy for a Common Identification Standard for Federal Employees and Contractors.* (27 August 2004). HSPD-12 establishes a policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

(13) **Homeland Security Presidential Directive/HSPD-13.** *Maritime Security Policy* (21 December 2004). HSPD-13 establishes US policy, guidelines, and implementation actions to enhance US national security and homeland security by protecting US maritime interests.

(14) **Presidential Decision Directive 39, US Policy On Counterterrorism.** PDD-39 validates and reaffirms existing federal lead agency responsibilities for counterterrorism, which are assigned to DOJ, as delegated to the FBI, for threats or acts of terrorism within the United States. The FBI as the LFA for CrM will involve only those federal agencies required and designated. The Directive further states that DHS/FEMA with the support of all agencies in the NRP, will support the FBI until the Attorney General transfers lead agency to DHS/FEMA. DHS/FEMA retains responsibility for CM throughout the response.

(15) **Presidential Decision Directive 62, Combating Terrorism** (pre-September 11, 2001) created a systematic approach to addressing the terrorist threat by reinforcing the mission of those agencies charged with fighting terrorism. The directive codified agency activities for apprehension and prosecution of terrorists, increased transportation security, enhanced response capabilities, and increased protection of computer-based systems that lie at the heart of the economy.

(16) **Executive Order 13231, Critical Infrastructure Protection in the Information Age,** established the President's Critical Infrastructure Protection Board and authorized a protection program to secure information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems.

(17) **The National Strategy for Homeland Security.** Prepared for the President by the Office of Homeland Security, this document lays out the strategic objectives, organization and critical areas for HS. The strategy identifies critical areas that focus on preventing terrorist attacks, reducing the nation's vulnerabilities, minimizing the damage and recovering from attacks that do occur. These critical areas are compatible with the DOD framework for HS that is discussed in this publication.

(18) **The Homeland Security Act of 2002** established the Department of Homeland Security to coordinate all federal HS activities to protect the Nation against threats to the homeland. To better facilitate the overarching HS mission area, Congress established DHS by merging numerous agencies into a single department.

(19) **USA Patriot Act of 2001**, 24 October 2001. This act enhances domestic security against terrorism. It eases some of the restrictions on foreign intelligence gathering within the US and affords the US intelligence community greater access to information discovered during a criminal investigation.

(20) **The Robert T. Stafford Disaster Relief and Emergency Assistance Act** sets the policy of the Federal government to provide an orderly and continuing means of supplemental assistance to state and local governments in their responsibilities to alleviate the suffering and damage that result from major disasters or emergencies. It is the primary legal authority for federal participation in domestic disaster relief. Under the Stafford Act, the President may direct federal agencies, including DOD, to support disaster relief. DOD may be directed to provide assistance in one of three different scenarios: a Presidential declaration of a major disaster, a Presidential order to perform emergency work for the preservation of life and property, or a Presidential declaration of emergency.

(21) **The Economy Act (Title 31 USC 1535)**. The Economy Act permits one federal agency to request the support of another provided that the requested services cannot be obtained more cheaply or conveniently by contract. Under this act, an LFA may request the support of DOD without a Presidential declaration of an emergency as required by the Stafford Act.

(22) **National Strategy to Combat Weapons of Mass Destruction** states that nuclear, biological, and chemical weapons in the possession of hostile states and terrorists represent one of the greatest security challenges facing the United States and that we must pursue a comprehensive strategy to counter this threat in all of its dimensions. Three principal pillars are: counterproliferation to combat its use, nonproliferation to combat proliferation, and consequence management to respond to its use.

(23) **National Strategy for Combating Terrorism**. Expands on the National Strategy for Homeland Security and the National Security Strategy by expounding on the need to destroy terrorist organizations, win the war of ideas, and strengthen America's security at home and abroad. While the national strategy focuses on preventing terrorist attacks within the US, this strategy is more proactive and focuses on identifying and defusing threats before they reach our borders. The direct and continuous action against terrorist groups will disrupt, and over time, degrade and ultimately destroy their capability to attack the US.

(24) **National Strategy for the Physical Protection of Critical Infrastructure and Key Assets**. Defines the road ahead for a core mission area identified in the President's NSHS. It identifies a clear set of national goals and objectives to achieve our protection goals. The strategy identifies thirteen critical infrastructure sectors. Key asset protection represents a broad array of unique facilities, sites, and structures whose disruption or destruction could have significant consequences across multiple dimensions. Examples include, but are not limited to nuclear power plants, national monuments, and commercial centers where large numbers of people congregate.

(25) **National Strategy for Securing Cyberspace**. An implementing component of the NSHS, it engages and empowers Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact. This will require a coordinated and focused effort from our entire society — the federal, state, and local governments. This strategy outlines a framework for

organizing and prioritizing efforts. It also identifies steps that state and local governments, private companies and organizations, and individual Americans can take to improve our collective cyber security. It identifies three strategic objectives: prevent cyber attacks against American critical infrastructure, reduce national vulnerability to cyber attacks, and minimize damage and recovery time from cyber attacks that do occur.

(26) **Posse Comitatus Act (Title 18 USC, Section 1385).** This federal statute places strict limits on the use of military personnel for law enforcement. Enacted in 1878, the PCA prohibits the willful use of the US Army (and later, the US Air Force) for law enforcement duties, except as authorized by the President, Congress or the US Constitution, or in certain emergency situations. Although the PCA, by its terms, refers only to the Army and Air Force, DOD policy extends the prohibitions of the Act to US Navy and Marine Corps forces, as well. Specifically prohibited activities include: interdiction of a vehicle, vessel, aircraft, or similar activity; search and/or seizure; arrest, apprehension, “stop-and-frisk” detentions, and similar activities; and use of military personnel for surveillance or pursuit of individuals, or as undercover agents, informants, investigators, or interrogators. DODD 5525.5, *DOD Cooperation with Civilian Law Enforcement Officials*, sets forth several forms of assistance civilian authorities, which are allowed under the PCA. Exceptions to PCA include:

- (a) NG forces operating under state active duty or Title 32.
- (b) Federal troops acting pursuant to the presidential power to quell insurrection.
- (c) Aerial photographic and visual search and surveillance by military personnel.
- (d) Congressionally created “drug exception.”
- (e) The USCG when operating under Title 14 authority.

(27) **Title 10 USC (Armed Forces).** Title 10 provides guidance on the US Armed Forces. Guidance is divided into 5 subtitles. One on general military law and one each for the US Army, US Navy and US Marine Corps, the US Air Force and the Reserve Components. Chapter 18 (sections 371-382) of Title 10 is entitled and governs Military Support for Civilian Law Enforcement Agencies. Title 10 USC 375 directs SecDef to promulgate regulations that prohibit “direct participation by a member of the Army, Navy, Air Force, or Marine Corps in a search, seizure, arrest, or other similar activity unless participation in such activity by such member is otherwise authorized by law.”

(28) **Title 14, USC**, sections 2, 19, 89, 141, and 143 define the statutory authority of the USCG during HS missions.

(29) **Title 32 USC, National Guard.** Specifically, statutes in Title 32 USC authorize the use of federal funds to train NG members while they remain under the command and control of their respective state governors. In certain limited instances, specific statutory or Presidential authority allows for those forces to perform operational missions funded by the Federal government, while they remain



under the control of the governor. Examples of those exceptions include the employment of WMD-CSTs, civil defense missions, and the President of the United States-directed airport security mission.

(30) **The National Security Strategy and the National Military Strategy.** The NSS establishes broad strategic guidance for advancing US interests in the global environment through the instruments of national power. The NMS, derived from the NSS, focuses on how the Armed Forces of the United States will be employed to accomplish national strategic objective. The NSS and the NMS continue to reflect the first and fundamental commitment to defend the Nation against its adversaries.

(31) **4 Mar 2003, Memorandum of Understanding Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing.** This agreement provides a framework and guidance to govern information sharing, use, and handling among the following individuals and their agencies: Secretary of Homeland Security, Director of Central Intelligence, the Attorney General, and any other organization having federal law enforcement responsibilities (other than those that are part of the Department of Homeland Security). The agreement mandates minimum requirements for information sharing, use, and handling and for coordination and deconfliction of analytic judgments.

## 2. Department of Defense Policy and Guidance

a. **Implications.** Specific authorities for HS missions are contained in federal and state law and policy documents. These form the basis for the development of DOD guidelines. These guidelines are promulgated in a variety of methods that include national strategy documents, planning guidance, and DODDs. These policy documents are consistent with and complementary to the federal statutes and guidelines discussed earlier in this appendix. DODDs specifically address HD and CS missions.

b. **Key DOD Guidance.** The following discussion identifies a number of key documents to make commanders and planners more aware of material that may assist in the planning and execution of the HS mission areas.

(1) **Unified Command Plan.** The UCP provides basic guidance to all unified combatant commanders; establishes their missions, responsibilities, and force structure; delineates the general geographical AORs for geographic combatant commanders; and specifies functional responsibilities for functional combatant commanders.

(2) **Strategic Planning Guidance (SPG).** The SPG provides direction for DOD components to develop the Future Years Defense Program and the President's budget submission. The four defense policy goals are to assure, dissuade, deter, and decisively defeat. The goals are articulated in a planning construct of deterring forward and winning decisively while defending at home. The SPG additionally lists the priorities of SecDef: winning the Global War on Terrorism, strengthening combined/joint warfighting capabilities, transforming the joint force, optimizing intelligence capabilities, counterproliferation, improving force manning, developing and implementing new concepts for global engagement, strengthening our ability to fulfill our responsibilities in HS, streamlining DOD processes, and reorganizing DOD and the US Government to deal with pre-war opportunities and post-war responsibilities.

(3) **Contingency Planning Guidance.** The CPG reflects SecDef's written policy guidance to the CJCS for contingency planning. It is issued with the approval of the President after consultation with the CJCS, provides the focus for the guidance in the NSS and SPG, and is the principal source document for CJCSI 3110.01, *Joint Strategic Capabilities Plan*.

(4) **DODD 2000.12, DOD Antiterrorism Program.** This directive updates policies and assigns responsibilities for implementing the procedures for the DODAT program. It establishes CJCS as the principal advisor and focal point responsible to SecDef for DOD AT issues. It also defines the AT responsibilities of the Military Departments, commanders of combatant commands, defense agencies, and DOD field activities. Its guidelines are applicable for the physical security of all DOD activities both overseas and in the homeland.

(5) **DODD 2000.15, Support to Special Events.** DODD provides definitions for a special event and support and outlines policy guidelines and responsibilities for DOD support of special events. It allows for the DOD component to designate a special events coordinator who is charged with providing timely information and technical support to the Assistant Secretary of Defense for Homeland Defense.

(6) **DODD 3020.XX, Defense Critical Infrastructure (Draft).** This directive establishes policy and assigns responsibilities for DCI activities as they apply to DOD, and authorizes ASD(HD) to issue instructions and guidance for the implementation of this directive. (Note: This document is the basis of DCI-related language in this publication.) This publication (JP 3-26) will reflect the language in this DODD regardless of the status of the DODD when this publication is promulgated.

(7) **DODD 3025.1, Military Support to Civil Authorities.** DODD 3025.1 provides guidance on CS activities for disaster-related civil emergencies. The LFA may request DOD assistance for CS missions. All requests for DOD assistance enter through the EXECSEC. When imminently serious conditions resulting from any civil emergency or attack may require immediate action, local military commanders and responsible officials of the DOD components may take such actions as may be necessary to save lives, prevent human suffering, and mitigate great property damage.

(8) **DODD 3025.12, Military Assistance for Civil Disturbances.** DODD 3025.12 provides guidance on CS activities for civil disturbances and civil disturbance operations, including response to terrorist incidents, and covers the policy and procedures whereby the President is authorized by the Constitution and laws of the United States to employ the Armed Forces to suppress insurrections, rebellions, and domestic violence under various conditions and circumstances. Planning and preparedness by the Federal Government and the Department of Defense for civil disturbances are important due to the potential severity of the consequences of such events for the Nation and the population.

(9) **DODD 3025.15, Military Assistance to Civil Authorities (MACA).** This directive governs all DOD MACA, including support in connection with incidents involving an act or threat of terrorism. The employment of US military forces in response to acts or threats of domestic terrorism must be requested by the Attorney General and authorized by the President.

SecDef must approve all requests for assistance. CJCS assists SecDef in implementing the DOD operational response to acts or threats of terrorism.

(10) **DODD 3150.8, *DOD Response to Radiological Accidents***. This directive promulgates DOD policy and planning guidance to implement the FEMA Federal Radiological Emergency Response Plan.

(11) **DODD 5160.54, *Critical Asset Assurance Program***. This directive expands the requirement to identify critical assets and ensure their integrity, availability, survivability, and capability to support vital DOD missions across the full range of military operations. It provides for an integrated infrastructure vulnerability assessment and assurance program based on an analysis of identified critical assets. (Note: This DODD will be superseded by DODD 3020.XX.)

(12) **DODD 5200.27, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense, 7 January 1980***. This directive establishes the Defense Investigative Program general policy, limitations, procedures, and operational guidance pertaining to the collecting, processing, storing, and disseminating of information concerning persons and organizations not affiliated with the Department of Defense.

(13) **DODD 5525.5, *DOD Cooperation with Civilian Law Enforcement Officials***. This directive assigns responsibilities and provides policy and procedures to be followed with respect to support provided to federal, state and local law enforcement efforts.

(14) **Chairman of the Joint Chiefs of Staff Concept Plan 0500, *Military Assistance to Domestic Consequence Management Operations in Response to a Chemical, Biological, Radiological, Nuclear, or High-Yield Explosives Situation***. This plan provides SecDef with a wide range of military options to assist in the domestic CM operations in response to a CBRNE incident. It also informs geographic combatant commanders of the full range of their CM responsibilities and it provides information and guidance for the conduct of domestic CM operations.

(15) **CJCSI 3110.16, *Military Capabilities, Assets, and Units for Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives Consequence Management Operations***. This instruction identifies and describes specific military capabilities, assets, and units potentially available to support military CM operations in response to CBRNE incidents. Although an actual CBRNE incident would involve a large array of DOD assets, this instruction primarily focuses on CM technical support and capabilities that are not generally found throughout the force. This instruction lists selected CBRNE-CM capabilities, assets and units by Service.

(16) **CJCSI 3121.02, *Rules for the Use of Force by DOD Personnel Providing Support to Law Enforcement Agencies Conducting Counterdrug Operations in the United States***. This instruction establishes rules regarding the use of force by DOD personnel during military operations that provide support to law enforcement agencies conducting CD operations in the US. It does not apply to US military units or personnel while under OPCON or TACON to the USCG in support of CD operations and does not apply to DOD support to CD operations outside the land area, internal

waters, territorial sea, and airspace of the United States, as well as that of US territories, possessions, and commonwealths. Such operations are governed by Standing Rules of Engagement for US Forces or the Use of Force Policy issued by the Commandant, USCG, or other authorities.

(17) **CJCSI 3125.01, *Military Assistance to Domestic Consequence Management Operations in Response to a Chemical, Biological, Radiological, Nuclear, or High-Yield Explosives Situation***. This instruction provides operational and policy guidance and instructions for US military forces supporting domestic CM operations in preparation for responding to a CBRNE situation. This instruction only applies to domestic CM operations. This instruction is of specific importance to the geographic combatant commands with domestic CBRNE responsibilities.

(18) **CJCSI 3209.01, *Critical Infrastructure Protection (Draft)***. This instruction establishes policy, assigns duties and responsibilities, and provides definitions for critical infrastructure terms. It specifically outlines responsibilities of the Joint Staff, combatant commanders, and Service Chiefs.

(19) **CJCSI 3710.01A, *DOD Counterdrug Operational Support***. This instruction promulgates SecDef delegation of authority to approve certain CD operational support missions. It also provides, in accordance with the Fiscal Year 1991 National Defense Authorization Act, as amended, instruction on authorized types of DOD (Title 10) CD support to LFAs, other government agencies, and foreign nations.

Intentionally Blank

## APPENDIX B COMBAT SUPPORT AGENCIES AND CAPABILITIES

### 1. Introduction

a. Combat support agencies (CSAs) provide direct support to the combatant commands performing HS during wartime or emergency situations and are subject to evaluation by CJCS. Figure B-1 illustrates the seven combat support agencies within DOD.

b. The following addresses general and specific missions, functions, and capabilities of DOD CSAs in support of HS activities.

### 2. Defense Information Systems Agency

Defense Information Systems Agency (DISA) is responsible for planning, engineering, acquiring, fielding, and supporting global net-centric solutions and operating the Defense Information System Network to serve the needs of the President, Vice President, SecDef, and the other DOD components across the range of military operations. DISA has a number of core mission areas that include communications, joint command and control, defensive information

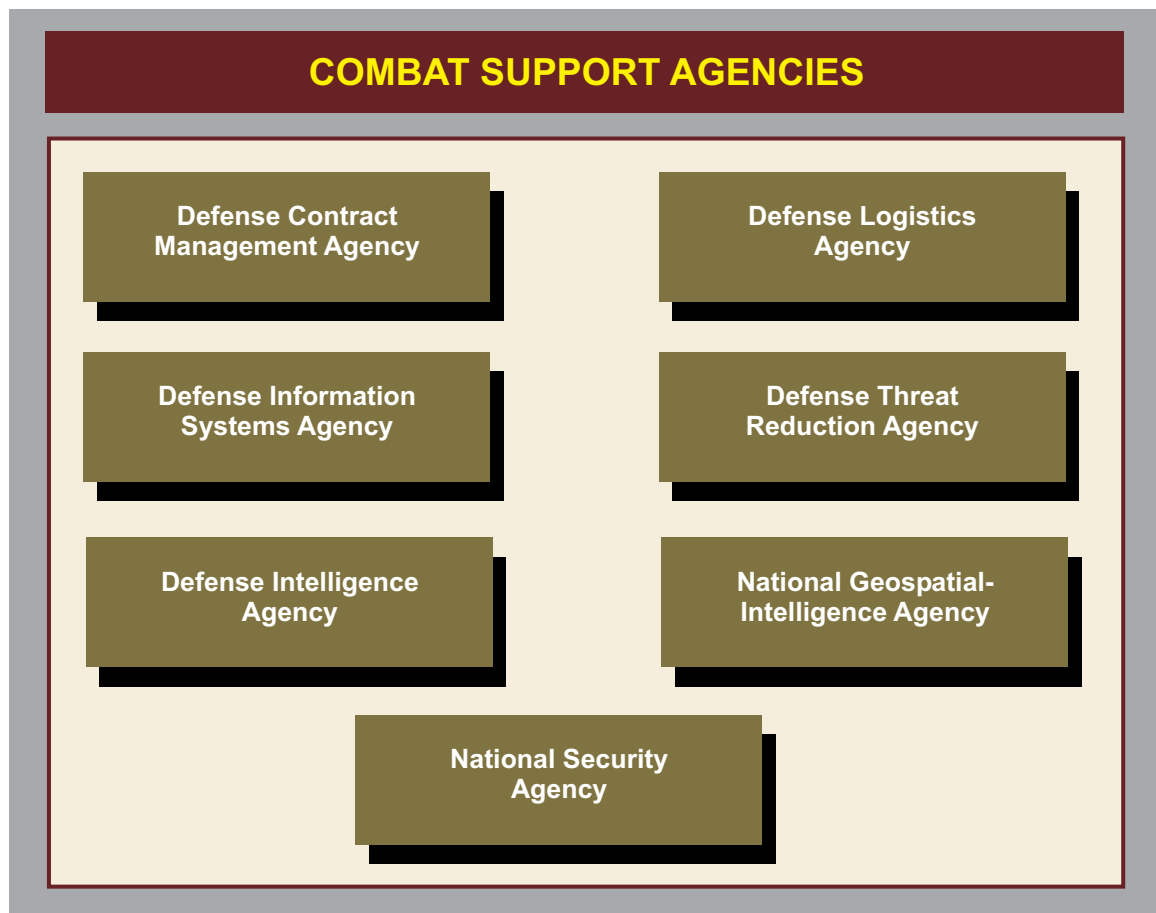


Figure B-1. Combat Support Agencies

operations, combat support computing, and joint interoperability support. For more information on DISA core missions, see its home page at [www.disa.mil](http://www.disa.mil).

### 3. Defense Intelligence Agency

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

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

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

d. DIA's Disruptive Technology Innovations Partnership (DTIP) program provides HD, and US infrastructure sectors with actionable information or time-sensitive intelligence assessments for correcting serious vulnerabilities. DTIP assessments prioritize vulnerabilities according to their national security impact were they to be exploited by state or non-state actors. DTIP assesses and warns of the impact of potential threats stemming from innovative applications of technologies against vulnerabilities.

e. DIA/J-2 has the ability to coordinate, establish, deploy, and operate a national intelligence support team (NIST) to the JTF-CS in support of HS. The NIST can deploy within 72 hours and will provide JTF-CS with national-level intelligence support in the areas of terrorism, FP and WMD.

### 4. Defense Logistics Agency

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

a. DLA provides logistic support to other DOD components and certain federal agencies, foreign governments, international organizations, and others as authorized.

b. DLA is headquartered at Fort Belvoir, Virginia. The DLA Director reports to the Under Secretary of Defense for Acquisition, Technology and Logistics through the Deputy Under Secretary of Defense (Logistics and Materiel Readiness).

c. DOD policy states that the primary means of supporting federally declared domestic emergencies is that other federal agencies have the lead and DOD has a supporting role. DLA must be prepared to provide support to supported combatant commanders or other Federal agencies.

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

e. The DLA Customer Handbook, a reference guide to everything DLA sells and supplies, is available at <http://www.supply.dla.mil/CustomerHandbook/index.asp>. A toll-free customer number is also available at 1-877-DLA-CALL.

## 5. National Security Agency

The resources of NSA are organized for the accomplishment of the following missions:

a. The IA mission provides the solutions, products and services, and conducts defensive IO, to achieve IA for information infrastructures critical to US national security interests.

b. The foreign signals intelligence or signals intelligence (SIGINT) mission allows 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 in accordance with objectives, requirements and priorities established by the Director, CIA with the advice of the National Foreign Intelligence Board.

c. NSA/Central Security Service executes SIGINT and information systems security activities and conducts related activities, as assigned by SecDef, including managing and providing operational control of the US SIGINT System. **Executive Order 12333 of 4 December 1981** describes in more detail the responsibilities of NSA.

## 6. Defense Contract Management Agency

Defense Contract Management Agency (DCMA) works directly with defense suppliers to help ensure that DOD, federal, and allied government supplies and services are delivered on time, at projected cost, and meet all performance requirements. DCMA performs all contract audits for DOD and provides accounting and financial advisory services regarding contracts and subcontracts to all DOD components responsible for procurement and contract administration. Within the DCIP, DCMA [subordinate to the



Under Secretary of Defense (Acquisition, Technology and Logistics)] is the DOD lead for the defense industrial base sector. For more information go to the DCMA webpage at [www.dcmamil](http://www.dcmamil).

### **7. National Geospatial-Intelligence Agency**

National Geospatial-Intelligence Agency (NGA) provides timely, relevant, and accurate geospatial intelligence (GEOINT) in support of national security objectives. GEOINT is the analysis and visual representation of security-related activities on the earth. NGA also:

a. Supports customers in the defense, law enforcement, intelligence, federal and civil communities for HS mission areas with its analytic GEOINT capabilities.

b. Supports defense missions for the COP, military operations assuredness, and FP by building integrated datasets to support the HS COP and situational awareness. These datasets will provide a common frame of reference for federal decision makers and operational planners for critical infrastructure vulnerability analysis and for domestic CrM and CM.

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

d. Provides integrated geospatial information in support of the planning and execution of HS exercises where there is federal, DOD, state and local government participation.

e. Deploys fully equipped geospatial analytic teams to support military and civilian exercises as well as other crisis and NSSEs in real time.

f. Provides direct, tailored geospatial information support.

g. Provides personnel as part of NISTs to USNORTHCOM, USPACOM, and DHS. These NISTs provide day-to-day GEOINT support to the command with the capability to reach back to NGA for requirements that exceed the capacity or capability of the team at the command.

### **8. Defense Threat Reduction Agency**

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

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

(1) Secure communications.

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

(3) Video and audio teleconferencing (secure and non-secure).

(4) Liaison and coordination of assistance from combatant commanders and other federal agencies in response to an accident or incident.

(5) Exchange of information with other agencies.

(6) Technical expertise, advice, and assistance, including targeting.

(7) Technical information, including data files on CBRNE materials.

(8) Data on effects of radiation on electronics.

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

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

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

(11) Nuclear forensics for Domestic Nuclear Event Attribution.

(12) Support to law enforcement investigations.

c. DTRA has a limited capability to deploy the following kinds of support assets:

(1) **Liaison Officers.** Already on-site at certain combatant commands. Additional LNOs could be dispatched to other commands as required.

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

(3) **Joint Staff Integrated Vulnerability Assessment Teams.** Assess mission survivability systems and architectures.

(4) **Balanced Survivability Assessment Teams.** Assess vulnerabilities of installations in terms of protecting people and missions from terrorist attack.

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

(6) **Site Assessment Teams.** Assess actual/potential CBRNE locations and facilities.

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

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

## APPENDIX C REFERENCES

The development of JP 3-26 is based on the following primary references:

### 1. General

- a. EO 12333, *United States Intelligence Activities*, 4 December 1981.
- b. EO 12656, *Assignment of Emergency Preparedness Responsibilities*, 18 November 1988.
- c. EO 13010, *Critical Infrastructure Protection*, 15 July 1996.
- d. EO 13228, *Establishing the Office of Homeland Security and the Homeland Security Council*, 8 October 2001.
- e. EO 13231, *Critical Infrastructure Protection in the Information Age*, 16 October 2001.
- f. *National Response Plan*, December 2004.
- g. HSPD-1, *Organization and Operations of the Homeland Security Council*, 29 October 2001.
- h. HSPD-2, *Combating Terrorism Through Immigration Policies*, 29 October 2001.
- i. HSPD-3, *Homeland Security Advisory System*, 11 March 2002.
- j. HSPD-4, *National Strategy to Combat Weapons of Mass Destruction*, December 2002.
- k. HSPD-5, *Management of Domestic Incidents*, 28 February 2003.
- l. HSPD-6, *Integration and Use of Screening Information*, 16 September 2003.
- m. HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*, 17 December 2003.
- n. HSPD-8, *National Preparedness*, 17 December 2003.
- o. HSPD-9, *Defense of United States Agriculture and Food*, 3 February 2004.
- p. HSPD-10, *Biodefense for the 21st Century*, 28 April 2004.
- q. HSPD-11, *Comprehensive Terrorist-Related Screening Procedures*, 27 August 2004.

- r. HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, 27 August 2004.
- s. HSPD-13, *Maritime Security Policy*, 21 December 2004.
- t. National Military Strategy, 11 September 2003.
- u. NSPD-1, *Organization of the National Security Council System*, 13 February 2001.
- v. NSPD-23, *National Policy on Ballistic Missile Defense*, 16 December 2002.
- w. National Security Strategy, September 2002.
- x. National Strategy for Homeland Security, July 2002.
- y. National Strategy for Physical Protection of Critical Infrastructure and Key Assets, February 2003.
- z. National Strategy for Combating Terrorism, February 2003.
- aa. The NORAD Agreement and Terms of Reference, and the CANUS Basic Security Document 100/35.
- bb. PDD-14, *Counternarcotics*, 3 November 1993.
- cc. PDD-39, *US Policy on Counterterrorism*, 21 June 1995.
- dd. PDD-62, *Combating Terrorism*, 22 May 1998. (*Unclassified Fact Sheet*).
- ee. PDD-NSC-67, *Enduring Constitutional Government and Continuity of Government Operations*, 21 October 1998.
- ff. Title 10, USC, *Armed Forces*.
- gg. Title 14, USC, *United States Coast Guard*.
- hh. Title 18, USC, Section 1385, *The Posse Comitatus Act*, 1878.
- ii. Title 31, USC, Section 1535, *The Economy Act*.
- jj. Title 32, USC, *National Guard*.
- kk. Title 42, USC, Section 5121, *The Stafford Act, as amended*, 20 October 2000.
- ll. The Homeland Security Act of 2002, 25 November 2002.

mm. The National Defense Authorization Act of 2002, 2 December 2002.

nn. Unified Command Plan 2002 with changes.

oo. United States Government Interagency Domestic Terrorism Concept of Operations Plan, January 2001.

## 2. Department of Defense

a. Department of Defense Civil Disturbance Plan: Garden Plot.

b. Secretary of Defense Message 1511147Z Nov 01, Policy Guidance — Impact of USA Patriot Act of 2001 on DOD Intelligence Activities and Intelligence Oversight.

c. DODD 2000.12, *DOD Antiterrorism (AT) Program*, 18 August 2003.

d. DODD 2000.15, *Support to Special Events*, 21 November 1994.

e. DODD 3020, *Defense Critical Infrastructure Program* (Draft, 15 June 2004).

f. DODD 3020.26, *Defense Continuity Program*, 8 September 2004.

g. DODD 3020.36, *Assignment of National Security Emergency Preparedness (NSEP) Responsibilities to DOD Components*, 2 November 1988.

h. DODD 3025.1, *Military Support to Civil Authorities*, 15 January 1993.

i. DODD 3025.12, *Military Assistance for Civil Disturbances*, 4 February 1994.

j. DODD 3025.15, *Military Assistance to Civil Authorities*, 18 February 1997.

k. DODD 3150.5, *DOD Response to Improvised Nuclear Device (IND) Incidents*, 24 March 1987.

l. DODD 5100.1, *Functions of the Department of Defense and Its Major Components*, 1 August 2002.

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

n. DODD 5240.1, *DOD Intelligence Activities*, 25 April 1988.

o. DODD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons*, December 1982.

p. DODD 5525.5, *DOD Cooperation with Civilian Law Enforcement Officials*, 15 January 1986.

q. DODI 3020, *Implementation of the Critical Infrastructure Program. (Draft)*

r. Strategic Planning Guidance.

s. Contingency Planning Guidance.

t. Quadrennial Defense Review.

### 3. Joint Publications

a. JP 1, *Joint Warfare of the Armed Forces of the United States*.

b. JP 0-2, *Unified Action Armed Forces*.

c. JP 1-02, *DOD Dictionary of Military and Associated Terms*.

d. JP 1-05, *Religious Ministry Support for Joint Operations*.

e. JP 2-0, *Doctrine for Intelligence Support to Joint Operations*.

f. JP 2-02, *National Intelligence Support to Joint Operations*.

g. JP 3-0, *Doctrine for Joint Operations*.

h. JP 3-01, *Joint Doctrine for Countering Air and Missile Threats*.

i. JP 3-01.1, *Aerospace Defense of North America*.

j. JP 3-01.5, *Doctrine for Joint Theater Missile Defense*.

k. JP 3-07, *Joint Doctrine for Military Operations Other Than War*.

l. JP 3-07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism*.

m. JP 3-07.4, *Joint Counterdrug Operations*.

n. JP 3-08 (Vols I & II), *Interagency Coordination During Joint Operations*.

o. JP 3-10.1, *Joint Tactics, Techniques, and Procedures for Base Defense*.

- p. JP 3-11, *Joint Doctrine for Operations in Nuclear, Biological, and Chemical (NBC) Environments.*
- q. JP 3-13, *Joint Doctrine for Information Operations.*
- r. JP 3-14, *Joint Doctrine for Space Operations.*
- s. JP 3-26.1, *Joint Doctrine for Homeland Defense. (TBP)*
- t. JP 3.26.2, *Joint Doctrine for Civil Support. (Draft)*
- u. JP 3-30, *Command and Control for Joint Air Operations.*
- v. JP 3-31, *Command and Control for Joint Land Operations.*
- w. JP 3-33, *Joint Force Capabilities.*
- x. JP 3-34, *Engineer Doctrine for Joint Operations.*
- y. JP 3-52, *Doctrine for Joint Airspace Control in the Combat Zone.*
- z. JP 3-53, *Doctrine for Joint Psychological Operations.*
- aa. JP 3-54, *Joint Doctrine for Operations Security.*
- bb. JP 3-61, *Doctrine for Public Affairs in Joint Operations.*
- cc. JP 4-0, *Doctrine for Logistic Support of Joint Operations.*
- dd. JP 4-02, *Doctrine for Health Service Support in Joint Operations.*
- ee. JP 4-04, *Joint Doctrine for Civil Engineering Support.*
- ff. JP 5-0, *Doctrine for Planning Joint Operations.*
- gg. JP 5-00.1, *Joint Doctrine for Campaign Planning.*
- hh. JP 5-00.2, *Joint Task Force Planning Guidance and Procedures.*
- ii. JP 6-0, *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations.*
- jj. Joint Military Operations Historical Collection.



kk. Domestic Operational Law (DOPLAW) Handbook for Judge Advocates.

ll. (TS) CJCSI 3110.01, *Joint Strategic Capabilities Plan FY 2002*, 1 October 2002.

mm. CJCSI, 3110.16, *Military Capabilities, Assets, and Units for Chemical, Biological, Radiological, Nuclear, and High Yield Explosive Consequence Management Operations*, 10 November 2000 (FOUO).

nn. CJCSI 3121.01A, *Standing Rules of Engagement for US Forces (U)*, 15 January 2000, document is classified SECRET.

oo. CJCSI 3121.02, *Rules on the Use of Force by DOD Personnel Providing Support to Law Enforcement Agencies Conducting Counterdrug Operations in the United States*, 31 May 2000.

pp. CJCSI 3125.01, *Military Assistance to Domestic Consequence Management Operations in Response to a Chemical, Biological, Radiological, Nuclear, or High-Yield Explosive Situation*, 3 August 2001.

qq. CJCSI 3209.01, *Critical Infrastructure Protection (CIP)*. (Draft)

rr. CJCSI 3214.01A, *Military Support to Foreign Consequence Management Operations*, 1 April 2003.

ss. CJCSI 3217.01A, *Military Assistance to the US Postal Service*, 1 October 1999.

tt. CJCSI 3710.01A, *DOD Counterdrug Support*, 30 March 2004.

uu. CJCSI 5113.02A, *Chairman of the Joint Chiefs of Staff Counterproliferation Charter (U)*, 10 August 2000, document is classified SECRET.

vv. CJCSI 5120.02, *Joint Doctrine Development System*.

#### 4. Army Publications

a. Field Manual (FM) 1, *The Army*, 14 June 2001.

b. FM 3-0, *Operations*, 14 June 2001.

c. FM 3-11.21/MCRP 3-37.2c/NTTP 3-11.24/AFTP(i) 3-2, *Multiservice Tactics, Techniques, and Procedures for Nuclear, Biological, and Chemical Aspects of Consequence Management*, 12 December 2001.

**5. Navy Publications**

Naval Doctrine Publication 1, *Naval Warfare*, 28 March 1994.

**4. Marine Corps Publications**

Marine Corps Doctrinal Publication 1, *Warfighting*, 6 March 1989.

**5. Air Force Publications**

a. Air Force Doctrine Document (AFDD) 1, *Air Force Basic Doctrine*, September 1997.

b. AFDD 2-4.2, *Health Services*.

c. AFTTP 3-42.32, *Home Station Response to CBRNE Events*.

**6. Coast Guard Publications**

a. Coast Guard Publication-1, *US Coast Guard: America's Maritime Guardian*.

b. Coast Guard Publication 3-01, *Maritime Strategy for Homeland Security*.

Intentionally Blank

## APPENDIX D ADMINISTRATIVE INSTRUCTIONS

### 1. User Comments

Users in the field are highly encouraged to submit comments on this publication to: Commander, United States Joint Forces Command, Joint Warfighting Center ATTN: Doctrine and Education Group, 116 Lake View Parkway, Suffolk, VA 23435-2697. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

### 2. Authorship

The lead agent for this publication is USNORTHCOM. The Joint Staff doctrine sponsor for this publication is the Director for Operations (J-3).

### 3. Change Recommendations

- a. Recommendations for urgent changes to this publication should be submitted:

TO: CSA WASHINGTON DC//DAMO-SSP//  
INFO: JOINT STAFF WASHINGTON DC//J7-JEDD//  
CDR USJFCOM SUFFOLK VA//DOCGP//

Routine changes should be submitted electronically to Commander, Joint Warfighting Center, Doctrine and Education Group and info to the lead agent and the Director for Operational Plans and Joint Force Development (J-7), JEDD.

- b. When a Joint Staff directorate submits a proposal to the Chairman of the Joint Chiefs of Staff that would change source document information reflected in this publication, that directorate will include a proposed change to this publication as an enclosure to its proposal. The Military Services and other organizations are requested to notify the Director, J-7, Joint Staff, when changes to source documents reflected in this publication are initiated.

- c. Record of Changes:

CHANGE NUMBER	COPY NUMBER	DATE OF CHANGE	DATE ENTERED	POSTED BY	REMARKS
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____

### 4. Distribution of Printed Publications

- a. Additional copies of this publication can be obtained through Service publication centers listed below (initial contact) or USJFCOM in the event that the joint publication is not available from the Service.

b. Individuals and agencies outside the combatant commands, Services, Joint Staff, and combat support agencies are authorized to receive only approved joint publications and joint test publications. Release of any classified joint publication to foreign governments or foreign nationals must be requested through the local embassy (Defense Attaché Office) to DIA Foreign Liaison Office, PO-FL, Room 1E811, 7400 Defense Pentagon, Washington, DC 20301-7400.

c. Additional copies should be obtained from the Military Service assigned administrative support responsibility by DOD Directive 5100.3, 15 November 1999, *Support of the Headquarters of Unified, Specified, and Subordinate Joint Commands*.

Army: US Army AG Publication Center SL  
1655 Woodson Road  
Attn: Joint Publications  
St. Louis, MO 63114-6181

Air Force: Air Force Publications Distribution Center  
2800 Eastern Boulevard  
Baltimore, MD 21220-2896

Navy: CO, Naval Inventory Control Point  
700 Robbins Avenue  
Bldg 1, Customer Service  
Philadelphia, PA 19111-5099

Marine Corps: Commander (Attn: Publications)  
814 Radford Blvd, Suite 20321  
Albany, GA 31704-0321

Coast Guard: Commandant Coast Guard (G-OPD), US Coast Guard  
2100 2nd Street, SW  
Washington, DC 20593-0001

Commander  
USJFCOM JWFC Code JW2102  
Doctrine Division (Publication Distribution)  
116 Lake View Parkway  
Suffolk, VA 23435-2697

d. Local reproduction is authorized and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified joint publications must be in accordance with DOD Regulation 5200.1-R, *Information Security Program*.

## 5. Distribution of Electronic Publications

a. The Joint Staff will not print copies of electronic joint publications for distribution. Electronic versions are available at [www.dtic.mil/doctrine](http://www.dtic.mil/doctrine) (NIPRNET), or <http://nmcc20a.nmcc.smil.mil/dj9j7ead/doctrine/> (SIPRNET).

b. Only approved joint publications and joint test publications are releasable outside the combatant commands, Services, and Joint Staff. Release of any classified joint publication to foreign governments or foreign nationals must be requested through the local embassy (Defense Attaché Office) to DIA Foreign Liaison Office, PO-FL, Room 1E811, 7400 Pentagon, Washington, DC 20301-7400.

Intentionally Blank

## GLOSSARY

### PART I — ABBREVIATIONS AND ACRONYMS

AFDD	Air Force doctrine document
ANG	Air National Guard
AOR	area of responsibility
ARNG	Army National Guard
ASD(HA)	Assistance Secretary of Defense (Health Affairs)
ASD(HD)	Assistant Secretary of Defense (Homeland Defense)
ASD(RA)	Assistant Secretary of Defense (Reserve Affairs)
ASD (SO/LIC)	Assistant Secretary of Defense (Special Operations and Low Intensity Conflict)
AT	antiterrorism
BMD	ballistic missile defense
BTS	Border and Transportation Security (DHS)
C2	command and control
CBRNE	chemical, biological, radiological, nuclear, or high-yield explosives
CD	counterdrug
CDRNORAD	Commander, North American Aerospace Defense Command
CDRUSCENTCOM	Commander, US Central Command
CDRUSEUCOM	Commander, US European Command
CDRUSJFCOM	Commander, US Joint Forces Command
CDRUSNORTHCOM	Commander, US Northern Command
CDRUSPACOM	Commander, US Pacific Command
CDRUSSOCOM	Commander, US Special Operations Command
CDRUSSOUTHCOM	Commander, US Southern Command
CDRUSSTRATCOM	Commander, US Strategic Command
CDRUSTRANSCOM	Commander, US Transportation Command
CIA	Central Intelligence Agency
CIP	critical infrastructure protection
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CM	consequence management
CMOC	Cheyenne Mountain Operations Center
CNGB	Chief, National Guard Bureau
CNO	computer network operations
COCOM	combatant command (command authority)
COG	continuity of government
CONPLAN	concept plan
CONUS	continental United States
COOP	continuity of operations
COP	common operational picture



CPG	Contingency Planning Guidance
CrM	crisis management
CS	civil support
CSA	combat support agency
CT	counterterrorism
DCI	defense critical infrastructure
DCIP	Defense Critical Infrastructure Program
DCMA	Defense Contract Management Agency
DCO	defense coordinating officer
DCST	Defense Logistics Agency (DLA) contingency support team
DEA	Drug Enforcement Administration
DEST	domestic emergency support team
DHHS	Department of Health and Human Services
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DOE	Department of Energy
DOJ	Department of Justice
DTIP	Disruptive Technology Innovations Partnership (DIA)
DTRA	Defense Threat Reduction Agency
EO	executive order
EOD	explosive ordnance disposal
EP	emergency preparedness
EPA	Environmental Protection Agency
EXECSEC	executive secretary
FBI	Federal Bureau of Investigation
FCC	Federal coordinating center
FEMA	Federal Emergency Management Agency
FM	field manual
FP	force protection
GEOINT	geospatial intelligence
GSA	General Services Administration
HD	homeland defense
HS	homeland security
HSAC	Homeland Security Advisory Council
HSC	Homeland Security Council
HSPD	homeland security Presidential directive

---

IA	information assurance
IO	information operations
ISR	intelligence, surveillance, and reconnaissance
JA	judge advocate
JDOMS	Joint Director of Military Support
JFHQ-NCR	Joint Force Headquarters-National Capital Region
JFO	joint field office
JACG	joint interagency coordination group
JP	joint publication
JTF	joint task force
JTF-CS	Joint Task Force-Civil Support
JTF-N	Joint Task Force North
LEA	law enforcement agency
LFA	lead federal agency
LNO	liaison officer
MACA	military assistance to civil authorities
MACDIS	military assistance for civil disturbances
MOA	memorandum of agreement
MOU	memorandum of understanding
MSCA	military support to civil authorities
MSCLEA	military support to civilian law enforcement agencies
NCI&KA	national critical infrastructure and key assets
NG	National Guard
NGA	National Geospatial-Intelligence Agency
NIMS	National Incident Management System
NIST	national intelligence support team
NMCC	National Military Command Center
NMS	national military strategy
NORAD	North American Aerospace Defense Command
NRP	National Response Plan
NSA	National Security Agency
NSC	National Security Council
NSHS	National Strategy for Homeland Security
NSPD	national security Presidential directive
NSS	national security strategy
NSSE	national special security event
OPCON	operational control
OPSEC	operations security

---

## Glossary

---

PA	public affairs
PAO	public affairs officer
PCA	Posse Comitatus Act
PDD	Presidential decision directive
POE	port of embarkation
PSYOP	psychological operations
RC	Reserve Component
RFA	request for assistance
ROE	rules of engagement
RUF	rules for the use of force
SecDef	Secretary of Defense
SECNAV	Secretary of the Navy
SIGINT	signals intelligence
SJFHQ-N	Standing Joint Force Headquarters - North
SPG	strategic planning guidance
TACON	tactical control
UCP	Unified Command Plan
USAFR	United States Air Force Reserve
USAR	United States Army Reserve
USC	United States Code
USCENTCOM	United States Central Command
USCG	United States Coast Guard
USCGR	United States Coast Guard Reserve
USDA	United States Department of Agriculture
USD(P)	Under Secretary of Defense for Policy
USEUCOM	United States European Command
USJFCOM	United States Joint Forces Command
USMCR	United States Marine Corps Reserve
USNORTHCOM	United States Northern Command
USNR	United States Navy Reserve
USPACOM	United States Pacific Command
USSOUTHCOM	United States Southern Command
USSS	United States Secret Service
USSTRATCOM	United States Strategic Command
WMD	weapons of mass destruction
WMD-CST	weapons of mass destruction-civil support team

## PART II — TERMS AND DEFINITIONS

**air defense.** All defensive measures designed to destroy attacking enemy aircraft or missiles in the Earth's envelope of atmosphere, or to nullify or reduce the effectiveness of such attack. Also called AD. (JP 1-02)

**antiterrorism.** Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces. Also called AT. See also counterterrorism; terrorism. (JP 1-02)

**chemical, biological, radiological, nuclear, or high-yield explosives incidents.** An emergency resulting from the deliberate or unintentional, release of nuclear, biological, radiological, or toxic or poisonous chemical materials, or the detonation of a high-yield explosive. Also called CBRNE incidents. (Approved for inclusion in the next edition of JP 1-02.)

**civil authorities.** Those elected and appointed officers and employees who constitute the government of the United States, of the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, United States possessions and territories, and political subdivisions thereof. (This term and its definition modify the existing term "United States Civil Authorities" and its definition and are approved for inclusion in the next edition of JP 1-02.)

**civil defense.** All those activities and measures designed or undertaken to: a. minimize the effects upon the civilian population caused or which would be caused by an enemy attack on the United States; b. deal with the immediate emergency conditions that would be created by any such attack, and c. effectuate emergency repairs to, or the emergency restoration of, vital utilities and facilities destroyed or damaged by any such attack. (JP 1-02)

**civil defense emergency.** See domestic emergencies. (JP 1-02)

**civil disturbance.** Group acts of violence and disorder prejudicial to public law and order. See also domestic emergencies. (JP 1-02)

**civil support.** Department of Defense support to US civil authorities for domestic emergencies, and for designated law enforcement and other activities. Also called CS. (Approved for inclusion in the next edition of JP 1-02.)

**combating terrorism.** Actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), taken to oppose terrorism throughout the entire threat spectrum. Also called CBT. See also antiterrorism; counterterrorism. (JP 1-02)

**common operational picture.** A single identical display of relevant information shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situational awareness. Also called COP. (JP 1-02)

**consequence management.** Actions taken to maintain or restore essential services and manage and mitigate problems resulting from disasters and catastrophes, including natural, manmade, or terrorist incidents. Also called CM. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

**continuity of operations.** The degree or state of being continuous in the conduct of functions, tasks, or duties necessary to accomplish a military action or mission in carrying out the national military strategy. It includes the functions and duties of the commander, as well as the supporting functions and duties performed by the staff and others acting under the authority and direction of the commander. Also called COOP. (JP 1-02.)

**counterdrug operations.** Civil or military actions taken to reduce or eliminate illicit drug trafficking. (JP 1-02)

**counterintelligence.** Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. Also called CI. (JP 1-02)

**counterterrorism.** Operations that include the offensive measures taken to prevent, deter, preempt, and respond to terrorism. Also called CT. See also antiterrorism; combating terrorism; terrorism. (JP 1-02)

**crisis management.** Measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or an act of terrorism. It is predominantly a law enforcement response, normally executed under federal law. Also called CrM. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

**critical asset.** A specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation to continue to function effectively. (Approved for inclusion in the next edition of JP 1-02.)

**critical infrastructure protection.** Actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Depending on the risk, these actions could include: changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding, etc. Also called CIP. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02)

**defense coordinating officer.** A military or civilian official who has been designated by the Department of Defense to exercise some delegated authority of the Department of Defense executive agent to coordinate military support to civil authorities activities. Also called DCO. (Approved for inclusion in the next edition of JP 1-02.)

**defense critical infrastructure.** Department of Defense and non-Department of Defense networked assets essential to project, support, and sustain military forces and operations worldwide. Also called DCI. (Approved for inclusion in the next edition of JP 1-02.)

**defense industrial base.** The Department of Defense, government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements. (Approved for inclusion in the next edition of JP 1-02.)

**defense sectors.** An identified grouping of Department of Defense functions that perform essential services required for military operations and the ability to project and support forces worldwide. (Approved for inclusion in the next edition of JP 1-02.)

**Department of Defense installation.** A facility subject to the custody, jurisdiction, or administration of any Department of Defense component. This term includes, but is not limited to, military reservations, installations, bases, posts, camps, stations, arsenals, vessels/ships, or laboratories where a Department of Defense component has operational responsibility for facility security and defense. (This term and its definition modify the existing term “military installation” and its definition and are approved for inclusion in the next edition of JP 1-02.)

**designated planning agent.** The commander responsible for planning, coordinating, and executing military taskings in civil emergencies for a particular branch or agency of the Department of Defense. (Approved for inclusion in the next edition of JP 1-02.)

**domestic emergencies.** Emergencies affecting the public welfare and occurring within the 50 states, District of Columbia, Commonwealth of Puerto Rico, US possessions and territories, or any political subdivision thereof, as a result of enemy attack, insurrection, civil disturbance, earthquake, fire, flood, or other public disasters or equivalent emergencies that endanger life and property or disrupt the usual process of government. The term “domestic emergencies” includes any or all of the emergency conditions defined below: a. civil defense emergency — A domestic emergency disaster situation resulting from devastation created by an enemy attack and requiring emergency operations during and following that attack. It may be proclaimed by appropriate authority in anticipation of an attack. b. civil disturbances — Riots, acts of violence, insurrections, unlawful obstructions or assemblages, or other disorders prejudicial to public law and order. The term “civil disturbance” includes all domestic conditions requiring or likely to require the use of Federal Armed Forces pursuant to the provisions of 10 USC 15. c. major disaster — Any flood, fire, hurricane, tornado, earthquake, or other catastrophe which, in the determination of the President, is or threatens to be of sufficient severity and magnitude to warrant disaster assistance by the Federal Government under Public Law 606, 91st Congress (42 USC 58) to supplement the efforts and available

resources of State and local governments in alleviating the damage, hardship, or suffering caused thereby. d. natural disaster — All domestic emergencies except those created as a result of enemy attack or civil disturbance. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

**domestic support operations.** None. (Approved for removal from the next edition of JP 1-02.)

**emergency preparedness.** Measures taken in advance of an emergency to reduce the loss of life and property and to protect a nation's institutions from all types of hazards through a comprehensive emergency management program of preparedness, mitigation, response, and recovery. Also called EP. (Approved for inclusion in the next edition of JP 1-02.)

**environmental considerations.** The spectrum of environmental media, resources, or programs that may impact on, or are affected by, the planning and execution of military operations. Factors may include, but are not limited to, environmental compliance, pollution prevention, conservation, protection of historical and cultural sites, and protection of flora and fauna. (JP 1-02)

**execute order.** 1. An order issued by the Chairman of the Joint Chiefs of Staff, by the authority and at the direction of the Secretary of Defense, to implement a decision by the President or Secretary of Defense to initiate military operations. 2. An order to initiate military operations as directed. Also called EXORD. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

**executive agent.** A term used to indicate a delegation of authority by the Secretary of Defense to a subordinate to act on the Secretary's behalf. Designation as executive agent, in and of itself, confers no authority. The exact nature and scope of the authority delegated must be stated in the document designating the executive agent. An executive agent may be limited to providing only administration and support or coordinating common functions, or it may be delegated authority, direction, and control over specified resources for specified purposes. Also called EA. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

**force protection.** Actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporates the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the enemy. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease. Also called FP. (JP 1-02)

**homeland.** The physical region that includes the continental United States, Alaska, Hawaii, United States territories and possessions, and surrounding territorial waters and airspace. (Approved for inclusion in the next edition of JP 1-02.)

**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. The Department of Defense is responsible for homeland defense. Homeland defense includes missions such as domestic air defense. The Department recognizes that threats planned or inspired by “external” actors may materialize internally. The reference to “external threats” does not limit where or how attacks could be planned and executed. The Department is prepared to conduct homeland defense missions whenever the President, exercising his constitutional authority as Commander in Chief, authorizes military actions. Also called HD. (Approved for inclusion in the next edition of JP 1-02.)

**homeland security.** Homeland security, as defined in the National Strategy for Homeland Security, is a concerted national effort to prevent terrorist attacks within the United States, reduce America’s vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. The Department of Defense contributes to homeland security through its military missions overseas, homeland defense, and support to civil authorities. Also called HS. (Approved for inclusion in the next edition of JP 1-02.)

**immediate response.** Any form of immediate action taken to assist civil authorities or the public to save lives, prevent human suffering, or mitigate great property damage under imminently serious conditions when time does not permit approval from a higher authority. (Approved for inclusion in the next edition of JP 1-02.)

**incident management.** A national comprehensive approach to preventing, preparing for, responding to, and recovering from terrorist attack, major disasters, and other emergencies. Incident management includes measures and activities performed at the local, state, and national levels and includes both crisis and consequence management activities. (Approved for inclusion in the next edition of JP 1-02.)

**information operations.** Actions taken to affect adversary information and information systems while defending one’s own information and information systems. Also called IO. (JP 1-02)

**instruments of national power.** All of the means available to the government in its pursuit of national objectives. They are expressed as diplomatic, economic, informational, and military. (This term and its definition modify the existing term “elements of national power” and its definition and are approved for inclusion in the next edition of JP 1-02.)

**interagency coordination.** Within the context of Department of Defense involvement, the coordination that occurs between elements of Department of Defense, and engaged US Government agencies, nongovernmental organizations, and regional and international organizations for the purpose of accomplishing an objective. (JP 1-02)



**joint regional defense command.** None. (Approved for removal from the next edition of JP 1-02.)

**joint state area command.** None. (Approved for removal from the next edition of JP 1-02.)

**law enforcement agency.** Any of a number of agencies (outside the Department of Defense) chartered and empowered to enforce US laws in the following jurisdictions: The United States, a state (or political subdivision) of the United States, a territory or possession (or political subdivision) of the United States, or within the borders of a host nation. Also called LEA. (JP 1-02)

**lead federal agency.** The federal agency that leads and coordinates the overall federal response to an emergency. Designation and responsibilities of a lead federal agency vary according to the type of emergency and the agency's statutory authority. Also called LFA. (Approved for inclusion in the next edition of JP 1-02.)

**major disaster.** See domestic emergencies. (JP 1-02)

**maritime domain.** All United States ports, inland waterways, harbors, navigable waters, Great Lakes, territorial seas, contiguous waters, customs waters, coastal seas, littoral areas, the United States Exclusive Economic Zone, and oceanic regions of United States national interest, as well as the sea lanes of communications to the United States, United States maritime approaches, and the high seas surrounding America. (This term and its definition are only applicable within the context of this publication and cannot be referenced outside this publication.)

**military assistance for civil disturbances.** A mission of civil support involving Department of Defense support, normally based on the direction of the President, to suppress insurrections, rebellions, and domestic violence, and provide federal supplemental assistance to the states to maintain law and order. Also called MACDIS. (Approved for inclusion in the next edition of JP 1-02.)

**military assistance to civil authorities.** The broad mission of civil support consisting of the three mission subsets of military support to civil authorities, military support to civilian law enforcement agencies, and military assistance for civil disturbances. Also called MACA. (Approved for inclusion in the next edition of JP 1-02.)

**military resources.** Military and civilian personnel, facilities, equipment, and supplies under the control of a Department of Defense component. (JP 1-02)

**military support to civil authorities.** A mission of civil support consisting of support for natural or man-made disasters, chemical, biological, radiological, nuclear, or high-yield explosive consequence management, and other support as required. Also called MSCA. (Approved for inclusion in the next edition of JP 1-02.)

**military support to civilian law enforcement agencies.** A mission of civil support that includes support to civilian law enforcement agencies. This includes but is not limited to: combating terrorism,

counterdrug operations, national security special events, and national critical infrastructure and key asset protection. Also called MSCLEA. (Approved for inclusion in the next edition of JP 1-02.)

**national critical infrastructure and key assets.** The infrastructure and assets vital to a nation's security, governance, public health and safety, economy, and public confidence. They include telecommunications, electrical power systems, gas and oil distribution and storage, water supply systems, banking and finance, transportation, emergency services, industrial assets, information systems, and continuity of government operations. Also called NCI&KA. (Approved for inclusion in the next edition of JP 1-02.)

**national emergency.** A condition declared by the President or the Congress by virtue of powers previously vested in them that authorize certain emergency actions to be undertaken in the national interest. Action to be taken may include partial, full, or total mobilization of national resources. (JP 1-02)

**primary agency.** The federal department or agency assigned primary responsibility for managing and coordinating a specific emergency support function in the National Response Plan. (Approved for inclusion in the next edition of JP 1-02.)

**rules for the use of force.** Directives issued to guide United States forces on the use of force during various operations. These directives may take the form of execute orders, deployment orders, memoranda of agreement, or plans. Also called RUF. (Approved for inclusion in the next edition of JP 1-02.)

**rules of engagement.** Directives issued by competent military authority that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered. Also called ROE. See also law of war. (JP 1-02)

**space defense.** None. (Approved for removal from the next edition of JP 1-02.)

**support agency.** A federal department or agency designated to assist a specific lead agency with available resources, capabilities, or expertise in support of emergency support response operations, as coordinated by the representative of the primary agency. See also lead federal agency. (Approved for inclusion in the next edition of JP 1-02.)

**supported commander.** 1. The commander having primary responsibility for all aspects of a task assigned by the Joint Strategic Capabilities Plan or other joint operation planning authority. In the context of joint operation planning, this term refers to the commander who prepares operation plans or operation orders in response to requirements of the Chairman of the Joint Chiefs of Staff.  
2. In the context of a support command relationship, the commander who receives assistance

from another commander's force or capabilities, and who is responsible for ensuring that the supporting commander understands the assistance required. (JP 1-02)

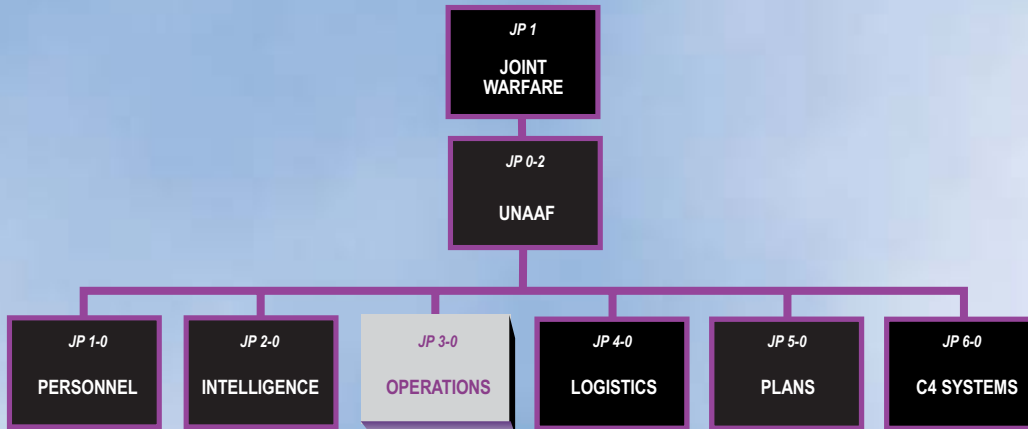
**supporting commander.** 1. A commander who provides augmentation forces or other support to a supported commander or who develops a supporting plan. Includes the designated combatant commands and Defense agencies as appropriate. 2. In the context of a support command relationship, the commander who aids, protects, complements, or sustains another commander's force, and who is responsible for providing the assistance required by the supported commander. (JP 1-02)

**technical operations.** Actions to identify, assess, dismantle, transfer, dispose of, or decontaminate personnel and property exposed during a chemical, biological, radiological, nuclear or high-yield explosive incident. (This term and definition is only applicable within the context of this publication and cannot be referenced outside this publication.)

**terrorism.** The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. See also antiterrorism; combating terrorism; counterterrorism. (JP 1-02)

**weapons of mass destruction.** Weapons that are capable of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people. Weapons of mass destruction can be high explosives or nuclear, biological, chemical, and radiological weapons, but exclude the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon. Also called WMD. (JP 1-02)

# JOINT DOCTRINE PUBLICATIONS HIERARCHY



All joint doctrine and tactics, techniques, and procedures are organized into a comprehensive hierarchy as shown in the chart above. **Joint Publication (JP) 3-26** is in the **Operations** series of joint doctrine publications. The diagram below illustrates an overview of the development process:

