Joint Doctrine for Homeland Security

Final Coordination
26 March 2004
1. Scope

This publication provides fundamental principles and doctrine to guide the Armed Forces in the conduct of homeland security operations in joint, multinational, and interagency environments. It describes the homeland security framework, mission areas, mission sets, and related incidents, supporting and enabling activities. It also discusses legal authorities, joint force and interagency relationships, command and control, planning and execution, 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 overarching doctrine to govern the joint activities and performance of the Armed Forces of the United States in joint operations and provides the doctrinal basis for interagency coordination and US military involvement in multinational and interagency operations. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders (JFCs) and prescribes doctrine for joint operations and training. It provides military guidance for use by the Armed Forces in preparing their applicable 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 deemed most appropriate to ensure unity of effort in the accomplishment of the overall mission.

3. Application

a. Doctrine and guidance established in this publication apply to the commanders of combatant commands, subunified commands, joint task forces, and subordinate components of these commands. These principles and guidance also may apply when significant forces of one Service are attached to forces of another Service or when significant forces of one Service support forces of another Service.

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 for the activities of joint forces unless the Chairman of the Joint Chiefs of Staff, normally in coordination with the other members of the Joint Chiefs of Staff, has provided more current and specific guidance. Commanders of forces operating as part of a multinational (alliance or coalition) military command should follow multinational doctrine and procedures ratified by the United States. For doctrine and procedures not ratified by the United States,
commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable and consistent with US law, regulations, and doctrine.

For the Chairman of the Joint Chiefs of Staff:

Timothy J. Keating
VADM, USN
Director, Joint Staff
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXECUTIVE SUMMARY ............................................................... TBP</td>
</tr>
<tr>
<td>CHAPTER I INTRODUCTION</td>
</tr>
<tr>
<td>• General ........................................................................ I-1</td>
</tr>
<tr>
<td>• Threats .......................................................................... I-55</td>
</tr>
<tr>
<td>• Global Security in Depth ................................................ I-89</td>
</tr>
<tr>
<td>• Department of Defense Homeland Security Objectives .......... I-161</td>
</tr>
<tr>
<td>• Department of Defense Homeland Security Operational Framework .......... I-691</td>
</tr>
<tr>
<td>• Legal and Policy Environment Considerations .................... I-1316</td>
</tr>
<tr>
<td>CHAPTER II COMMAND RELATIONSHIPS; AND INTERAGENCY RESPONSIBILITIES AND CONSIDERATIONS</td>
</tr>
<tr>
<td>• General ........................................................................ II-1</td>
</tr>
<tr>
<td>• Command and Control Relationships and Responsibilities ........ II-23</td>
</tr>
<tr>
<td>• Federal Agency Responsibilities and Considerations ............ II-1416</td>
</tr>
<tr>
<td>• Non-Department of Defense Federal Agencies and Responsibilities .... II-141720</td>
</tr>
<tr>
<td>CHAPTER III HOMELAND DEFENSE OPERATIONS</td>
</tr>
<tr>
<td>• General ........................................................................ III-1</td>
</tr>
<tr>
<td>• Homeland Defense Operational Elements and Characteristics .... III-42</td>
</tr>
<tr>
<td>• Homeland Defense Missions .............................................. III-4</td>
</tr>
<tr>
<td>• Common Functions Supporting Operations and Enabling Activities ........ III-56</td>
</tr>
<tr>
<td>• Planning Considerations for Homeland Defense Operations .......... III-912</td>
</tr>
<tr>
<td>CHAPTER IV CIVIL SUPPORT</td>
</tr>
<tr>
<td>• General ........................................................................ IV-1</td>
</tr>
<tr>
<td>• Civil Support Operational Elements and Characteristics ........ IV-23</td>
</tr>
<tr>
<td>• Civil Support Missions .................................................... IV-23</td>
</tr>
<tr>
<td>• Associated Supporting Operations and Enabling Terms Activities .......... IV-689</td>
</tr>
<tr>
<td>• Department of Defense Civil Support Process .................... IV-141012</td>
</tr>
<tr>
<td>• Request for Assistance Process ........................................ IV-912</td>
</tr>
<tr>
<td>• Authorities ...................................................................... IV-12</td>
</tr>
<tr>
<td>• Planning Considerations for Civil Support Operations .......... IV-136</td>
</tr>
</tbody>
</table>
## Table of Contents

1. **APPENDIX**

   A  Key Homeland Security Legal and Policy Documents ........................................... A-1
   B  Joint Education, Training, Exercises, and Simulations ........................................ B-1
   CB  Combat Support Agencies and Capabilities ...................................................... CB-1
   D  Key Federal Departments, Agencies, and Capabilities ....................................... D-1
   EC  References ...................................................................................................... EC-1
   FD  Administrative Instructions ............................................................................. FD-1

2. **GLOSSARY**

   Part I  Abbreviations and Acronyms..................................................................... GL-1
   Part II  Terms and Definitions ........................................................................... GL-63

3. **FIGURE**

   I-1  National Strategy for Homeland Security .................................................... I-3
   I-2  Operational Descriptions of Homeland Security and Mission Areas ............. I-34
   I-3  Relationship of Emergency Preparedness to Homeland Security Mission Areas I-345
   I-34  Homeland Security Strategic Threat Environment ......................................... I-456
   I-45  Critical Infrastructure Protection Framework ............................................... I-629
   I-56  Homeland Security Operational Framework .................................................. I-81213
   I-67  Homeland Security Campaign Model ............................................................ I-91416
   I-8  Sources of Guidance for the Homeland Security Mission ................................ I-17
   II-1  Geographic Combatant Command Areas of Responsibility ............................ II-2
   II-2  Organizational Chart: Office Department of the Assistant Secretary of Defense for Homeland Security Defense .......................................................... II-46
   II-3  US Northern Command Organization and Command Relationships ............. II-68
   II-4  Disaster Response Process ............................................................................. II-11
   II-54  Guidelines for Interagency Coordination ..................................................... II-121518
   II-6  FEMA Emergency Support Functions ........................................................... II-13
   II-5  Interagency Coordination .............................................................................. II-18
   II-56  Lead Federal Agency/Department of Defense Relationships ....................... II-151821
   II-867  Department of Homeland Security Organizational Structure .................... II-162022
   II-9  Local to Federal Response Chain .................................................................. II-19
   III-1  Homeland Defense Characteristics, and Missions, and Operational Elements III-2
   III-2  Homeland Defense Missions and Common Functions .................................. III-5
   III-3  Examples of Defense Critical Infrastructure Assets ..................................... III-7
   III-4  Example of a Campaign Model Addressing Homeland Defense Activities ...... III-9
   IV-1  Civil Support Missions and Functions ........................................................... IV-234
   IV-2  Examples of Military Support to Civil Authorities ......................................... IV-345
   IV-3  Military Support to Civilian Law Enforcement Agencies .............................. IV-36
   IV-4  Examples of National Critical Infrastructure ................................................ IV-57
   IV-53  Military Assistance for Civil Disturbance Operations .................................. IV-589
Table of Contents

<table>
<thead>
<tr>
<th>IV-64</th>
<th>Relationship Between Crisis Management and Consequence Management</th>
<th>IV-7910</th>
</tr>
</thead>
<tbody>
<tr>
<td>IV-7</td>
<td>Functional Line of Coordination Between the Office of the Secretary of Defense, the Joint Chiefs of Staff, and the Combatant Commanders: Request for Assistance</td>
<td>IV-811</td>
</tr>
<tr>
<td>IV-5</td>
<td>Examples of Critical Infrastructure</td>
<td>IV-12</td>
</tr>
<tr>
<td>IV-6</td>
<td>Request for Assistance</td>
<td>IV-13</td>
</tr>
<tr>
<td>IV-8</td>
<td>Example of DOD Response Chain for a Chemical, Biological, Radiological, Nuclear, High Yield Explosive Incident</td>
<td>IV-9</td>
</tr>
<tr>
<td>B-1</td>
<td>The Joint Training System</td>
<td>B-3</td>
</tr>
<tr>
<td>B-2</td>
<td>Example Homeland Security Training Program</td>
<td>B-5</td>
</tr>
<tr>
<td>B-3</td>
<td>Weapons of Mass Destruction Focused Exercise Training</td>
<td>B-8</td>
</tr>
<tr>
<td>B-4</td>
<td>Operational &amp; Planning Exercises for Command and Control Elements</td>
<td>B-9</td>
</tr>
<tr>
<td>CB-1</td>
<td>Defense-COMBAT Support Agencies</td>
<td>CB-1</td>
</tr>
</tbody>
</table>
Table of Contents

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

Intentionally Blank
EXECUTIVE SUMMARY
COMMANDER’S OVERVIEW

• Provides the strategic context for doctrinal guidance for homeland security mission areas of homeland defense and civil support

• Articulates the national strategy for homeland security

• Discusses Department of Defense contributions to the homeland security mission

• Describes the threat to the homeland and discusses global security in depth

• Defines the homeland and other key terms associated with homeland security

• Identifies operational elements and characteristics for homeland defense and civil support mission areas

• Describes command and control relationships for Department of Defense and non-Department of Defense activities associated with homeland security mission areas

• Describes key homeland security legal and policy documents

• Identifies the roles and capabilities of Department of Defense Combat Support Agencies

The Strategic Context

The homeland is described as the physical region that includes the continental United States (CONUS), Alaska, US territories and possessions, surrounding territorial waters and airspace. Homeland security is the Nation’s first priority.

The homeland is described as the physical region that includes the continental United States (CONUS), Alaska, US territories and possessions, surrounding territorial waters and airspace. The security of the homeland is the nation’s first priority and is a national effort. To preserve the freedoms guaranteed by the Constitution, the Nation must be protected from hostile state and non-state actor threats and violence, including terrorism. Department of Defense has a key role in the security of the homeland.
Executive Summary

The National Strategy

The Department of Homeland Security has the lead for the overarching homeland security mission.

The military instrument of national power is a critical enabler and is applied in concert with the other instruments of national power in our efforts to secure the homeland.


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 an understanding of the distinction between the role that the Department of Defense plays with respect to securing the homeland and that of the Department of Homeland Security.

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 broader role in detecting and preventing threats or acts of terrorism. Our national military objectives to defend the homeland will take in to account our national interests highlighted in the 2001 Quadrennial Defense Review and specifically our enduring interests of ensuring US security and freedom of action.

The NSHS identifies the following strategic objectives: preventing terrorist attacks, reducing our Nation’s vulnerabilities, minimizing the damage, and recovering from attacks that do occur. In order to ensure the security of the homeland, the following critical areas will require increased emphasis: intelligence and warning; border and transportation security; domestic counterterrorism; protecting national critical infrastructure and key assets (NCI/KA) protection; defense against catastrophic threats; international cooperation; interoperability; and emergency preparedness and response

Department of Defense Contributions

Armed Forces support national homeland security efforts through two distinct mission areas – homeland defense and civil support.

The Armed Forces support the HS strategy through two distinct but interrelated mission areas – homeland defense (HD) and civil support (CS). HS at the national level specifically focuses on terrorist threats. DOD’s approach to HS focuses on a broader range of threats and responses. DOD may serve as the lead or provide support to other federal agencies in their actions to secure the homeland.
Executive Summary

DOD serves as the lead for the HD mission area and supports other lead federal agencies for CS missions.

Homeland defense is the protection of US territory, sovereignty, domestic population, and defense critical infrastructure (DCI), against external threats and aggression. DOD is the lead federal agency for HD. The military role in the CS mission is DOD support to US civil authorities for domestic emergencies, and for designated law enforcement and other activities in accordance with US law. To ensure the Department’s readiness for both HD and CS missions, DOD must also engage in emergency preparedness activities. EP consists of those activities undertaken to ensure the military is prepared, trained and ready and that DOD processes, procedures and resources are in place to support the President, SecDef, and as required, other federal departments and agencies in a designated national security emergency.

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 security environment through the application of diplomatic, economic, military, informational, and cultural engagement. Internally, we have relied primarily on the justice system to provide for domestic peace and tranquility.

Global Security In Depth

Geographically DOD HS responsibilities encompass the forward regions, approaches, and the homeland itself. The dividing lines associated with these three regions are not absolute and they may overlap or shift based on the threat.

DOD’s HS responsibilities are global in nature and defenses are conducted in depth beginning at the source of the threat. The global approach to military HS responsibilities encompasses forward regions, approaches, and the homeland itself. It is important to note that the divisions among all three regions are not absolute and areas may overlap or shift depending on the situation and threat. Military operations associated with HS will therefore require thorough integration and synchronization. A global approach to HS includes deterrence, which encompasses actions such as certain overwhelming retaliation, preemptive activities that neutralize an adversary’s first strike capability, and defenses in depth that render any attack futile. In addition, a HS global approach must include preparation coordination and capabilities to mitigate the consequences of attacks even if partially successful.

Global Security In Depth

The overarching operational framework for DOD HS consists of two mission areas – HD and CS. Emergency preparedness activities are applied and exercised when conducting both missions.
There are three missions associated with homeland defense – air defense, land defense and maritime defense. Supporting operations and enabling activities span the scope of all three HD missions.

Employment of military forces under the auspices of civil support fall under the broad mission of military assistance to civil authorities (MACA). Subordinate missions under MACA consist of military assistance for civil disturbance, military support to civil authorities and military support to civil law enforcement agencies.

Command and control of the Armed Forces is exercised through two distinct chains of command.

The lead for each HD and CS mission will vary. Regardless of the mission area (HD or CS), military forces always remain under the control of a military chain of command.

The HD mission area consists of three missions: air defense, land defense, and maritime defense. HD missions consist of two operational elements: offensive actions — preemptive activities to deter, disrupt and destroy adversary capabilities at their source and defensive actions — passive and active defenses. The operational elements are coordinated, synchronized and integrated through command control, communications computers and intelligence systems. Supporting operations and enabling activities that may be applied to all HD missions include: critical infrastructure protection (CIP), AT and FP, space operations, ballistic missile defense and information operations (IO).

Employment of military forces within the US, its territories, and possessions provided under the auspices of CS, typically falls under the broad mission of military assistance to civil authorities (MACA). MACA operations consist of three subordinate missions: military assistance for civil disturbance (MACDIS), military support to civil authorities (MSCA), and military support to civil law enforcement agencies (MSCLEA). Supporting operations and enabling activities associated with the CS mission area include, but are not limited to domestic chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE), crisis management (CrM) and consequence management (CM), counterdrug operations, maritime security, NSSE support activities, disaster responses, border security, AT activities, intelligence sharing, EP activities, and IO.

Command and Control

The President exercises authority and control of the Armed Forces through two distinct branches of the chain of command. One branch runs from the President, through the Secretary of Defense to commanders of combatant commands. The other branch, used for purposes other than operational direction of forces, runs from the President through the Secretary of Defense to Secretaries of the Military Departments.

For homeland defense missions, DOD serves as the lead federal agency with other federal agencies in support. When conducting civil support missions, DOD will be in support of another lead federal agency. Regardless of whether Department of Defense is conducting homeland defense or civil support, military forces will always remain under the control of the established Title 10, 32, and / or State active duty military chain of command.
Executive Summary


Incident response inside the homeland will require close coordination and detailed information sharing among a variety of federal, state, and local agencies and organizations. Depending on the incident, the following departments and agencies, other than DOD, that form the core of participants serving as HS federal responders include: the Homeland Security Advisory Council, the Department of Homeland Security, the Department of Energy, the Department of Justice, the Environmental Protection Agency, the Department of Health and Human Services, the United States Department of Agriculture, the General Services Administration and the American Red Cross.

Key Policy Documents

There are a variety of documents that provide guidance for the homeland security mission. These range from the US Constitution to the Contingency Planning Guidance. Key executive and legislative guidance include: Homeland Security Presidential Directives, Presidential Decision Directives, legislative acts, national strategy documents, and United States Codes. Department of Defense policy and guidance is contained in plans, Department of Defense directives and instructions and Chairman of the Joint Chiefs of Staff instructions.

Combat Support Agencies

Combat support agencies provide direct support to the combatant commands performing HS during wartime or emergency situations and are subject to evaluation by the Chairman of the Joint Chiefs of Staff. The seven DOD combat support agencies are: the Defense Information Systems Agency, the Defense Threat Reduction Agency, the National Geospatial Agency, the National Security Agency, the Defense Logistics Agency, the Defense Intelligence Agency, and the Defense Contracting Management Agency.
Conclusion

The security of the homeland is the nation’s first priority and is a national effort. The Department of Homeland Security has the lead for the homeland security mission and DOD support to that effort is accomplished through two distinct mission areas—homeland defense and civil support. Emergency preparedness activities span national and DOD homeland security efforts and for DOD they are applied across both HD and CS missions. DOD exercises a global approach to HS and responsibilities encompass the forward regions, approaches, and the homeland itself. For homeland defense missions, DOD serves as the lead federal agency with other federal agencies in support. For civil support missions, DOD serves in supporting roles. Responses to HS incidents will require close coordination between all federal state and local participants. Synchronization and integration of DOD efforts is essential.
CHAPTER I
INTRODUCTION

“\textit{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.}”

\begin{flushright}
President George W. Bush
\end{flushright}

1. General

The homeland, described as the physical region that includes the continental United States (CONUS), Alaska, \textit{US} territories and possessions, surrounding territorial waters and airspace, and citizens of the United States are at all times exposed to the possibility of harm from hostile powers, states or non-state actors. Against such dangers, the Nation must be ever vigilant. To preserve the freedoms and way of life guaranteed by the Constitution of the United States, the Nation must have a homeland that is secure from adversary threats and violence, including terrorism. \textit{Homeland security (HS) is the Nation’s first priority, and it is a national effort.} The Armed Forces of the United States—Department of Defense (DOD) make critical contributions to that effort has a key role in that effort. They hold in trust for the American people the military power of the Nation and are the ultimate guarantors of its territorial integrity and independence against all adversaries. When called to action, they support and defend national interests worldwide. The National Security Strategy of the United States aims to guarantee the sovereignty and independence of the United States, with our fundamental values and institutions intact. It provides a framework for creating and seizing opportunities that strengthen our security and prosperity. 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. \textit{Critical to understanding the overall relationship is an understanding of the distinction between the role that the DOD plays with respect to securing the Nation and HS and that defined in the NSHS, which has the Department of Homeland Security (DHS) as the lead.}

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 broader role in detecting, and preventing, and deterring threats or acts of terrorism to our interests. Our national military objectives to defend the homeland will take in to account our enduring national interests highlighted in the 2001 Quadrennial Defense Review and specifically our enduring interests of ensuring US security and freedom of action, promote security and deter aggression, fight and win the Nation’s wars, and ensure military superiority are \textit{US security is the ends upon which the execution of our strategy is focused. Foreign-Adversary perceptions of US military}
capabilities and intent are fundamental to strategic deterrence. 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 National Strategy for Homeland Security—NSHS identifies the following
critical tasks:—strategic objectives: preventing terrorist attacks, reducing our Nation’s
vulnerabilities, minimizing the damage, and fostering recovery should such recovering
from attacks that do occur. In order to ensure the security of the homeland, the
following critical areas will require increased emphasis: intelligence and warning; border
and transportation security; domestic counterterrorism; protecting national critical
infrastructure (national and defense) and key assets (NCI/KA) protection; defense against
catastrophic threats; international cooperation; interoperability; and emergency
preparedness and response (Figure I-1).

(1) The Armed Forces support the national homeland security (HLS) strategy through
two distinct but interrelated mission areas—homeland defense (HLD) and civil support
(CS). The following descriptions of HLS and its two mission areas reflect a Department
of Defense (DOD) interpretation of the homeland security mission. The descriptions
provide an overarching perspective and do not necessarily identify all of the specific
actions performed by various agencies. The military application of the homeland
security strategy is the preparation for, deterrence of, preemption of, defense against, and
response to threats and aggression directed toward US infrastructure; as well as crisis
management (CrM), consequence management (CM), and other domestic CS. To
support the NSHS, the Armed Forces, in accordance with guidance established in the
National Military Strategy (NMS), conducts 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 HS strategy calls for preparation, detection, deterrence, preemption and the defeat of threats and aggression aimed at the homeland. DOD also provides military assistance to civil authorities, including consequence management activities. The Armed Forces support the HS strategy through two distinct but interrelated mission areas – homeland defense (HD) and civil support (CS). Figure I-2 reflects an overarching description for HS to include both that depicted in the NSHS and the DOD contribution. The descriptions for HD and CS depicted in the figure represent the DOD interpretation of its role in carrying out the HS strategy. The mission area descriptions provide an overarching perspective and do not necessarily identify all of the specific actions performed by various agencies. As depicted below, HS at the national level has a specific focus on terrorist threats. The DOD HS focus is broader.

(a) Homeland defense HD is the protection of US territory, sovereignty, domestic population, and DOD-defense critical infrastructure (DCI), including non-defense critical infrastructure dependencies and interdependencies, against external threats and aggression. DOD is the lead for HD.

(b) The military 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 Posse Comitatus and other

Figure I-1. National Strategy for Homeland Security
activities support approved by the Secretary of Defense (SecDef). SecDef provides military support to civil authorities for domestic incidents as directed by the President and consistent with military readiness, Department of Defense directives (DODDs), and the law.

The Secretary of Defense provides military support to civil authorities for domestic incidents as directed by the President and consistent with military readiness, DOD Directives, and the law.

(3) To ensure the Department’s readiness for homeland defense HD and civil support CS missions, DOD must also engage in emergency preparedness (EP). EP consists of those planning activities undertaken to ensure DOD processes, procedures and resources are in place to support the President and Secretary of Defense SecDef, and as required, other federal departments and agencies in a designated National Security Emergency. Emergency preparedness EP is considered a part of DOD’s overall preparedness activities. Within DOD, it is not considered a stand-alone activity, but is an integral part of training and preparation efforts. Figure I-3 reflects illustrates how HD, CS and EP are connected and related to national HS efforts this integration.
To orchestrate the myriad of capabilities associated with the National Strategy for Homeland Security NSHS, DOD must closely coordinate efforts with the Department of Homeland Security DHS, other federal, State, and local and other Federal government agencies, and facilitate information sharing to assure unity of effort. Since many homeland security 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, the Department of Homeland Security DHS coordinates federal activities, integrates national preparedness and response systems, and encourages development and enhancement of State and local capabilities.

2. Threats

Our Federal system was born, in part, out of a need to provide for the common defense. Americans have traditionally enjoyed great security from external threats. In recent history, no hostile powers have existed adjacent to our borders and the Nation has been insulated from attack by two vast oceans. In today's complex threat environment, our approach to security must continue to address both external and internal aspects. Externally, the United States US has sought to shape the international environment through the application of strong global political, diplomatic, economic, military, informational, and cultural engagement. Internally, we have relied primarily on the...
justice system to provide for domestic peace and tranquility. Recent attacks from both within and outside our borders have identified exposed vulnerabilities. Given the omnipresent persistent nature of current threats, a proactive, comprehensive approach to homeland security—HS is required. The uncertainty associated with these emerging conditions is reflected in the strategic environment faced by the Nation. This strategic environment is depicted in Figure I-4.

a. An adversary’s choice of weapons to threaten the US homeland range from conventional means to chemical, biological, radiological, nuclear or high-yield explosives (CBRNE). 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 or economic importance are within the capabilities of a number 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 chemical, biological radiological and nuclear weapons—weapons of mass destruction (WMD) and the means to deliver them. Terrorist attacks in the New York, Washington, Pennsylvania and Oklahoma City have highlighted adversary capabilities and asymmetric approaches. Successfully countering both traditional and asymmetric threats and reducing risk will require both a concerted and coordinated effort by the DOD and other

---

**HOMELAND SECURITY STRATEGIC THREAT ENVIRONMENT**

- Diminished protection afforded by geographic distances.
- Traditional threats remain.
- Greater risk of a weapons mass destruction attack.
- Increased potential for miscalculation and surprise.
- Increased potential for terrorist attacks.
- Increased challenges from weak and failing states and non-state actors.
- Increasing diversity in sources and unpredictability of the locations of conflict.
- Threats to US vital interests overseas.

---

**Figure I-4. Homeland Security Strategic Threat Environment**
Federal agencies as well as by state and local governments. Similar coordination will be required to successfully mitigate the consequences of attacks—even if partially successful.

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 is moved globally accessed. Adversaries have taken advantage of this technology and employ it in their own operations, be it such as moving money, communicating with cells in their organizations, approving missions, or conducting reconnaissance and surveillance on potential targets. A number of regional powers, non-state actors, and transnational groups already possess a capacity—the capability to challenge the interests of the United States US abroad as well as and those of its our allies. All are expected to continue improving their capabilities and seek an asymmetrical advantages against over the US and its our allies. The number of nations—adversaries that may effectively threaten our ability to protect our interests overseas is increasing at a rapid pace.

d. America remains vulnerable to large-scale terrorist attacks. Evidence suggests that terrorist organizations have grown more radical—extreme in their objectives and methods—actions and are less concerned that attacks on innocent civilians or public infrastructure will undermine support for their causes. Some have developed a considerable degree of fiscal independence and essentially are prone to “declare war” on the United States US with little regard as to how we will respond. See Joint Publication (JP) 3-07.2, Joint Tactics Techniques and Procedures for Antiterrorism Joint Tactics Techniques and Procedures for Antiterrorism for more information on terrorist threats.

*America remains vulnerable to large-scale terrorist attacks.*
e. In spite of intensive counterproliferation and arms control efforts, the likelihood that adversaries will attempt to employ weapons of mass destruction (WMD) against the US or its interests somewhere in the world has increased. A WMD attack, whether delivered conventionally by a known adversary using conventional means (missiles and bombers) or asymmetrically (employing terrorist tactics), could result in a number of consequences for the nation (e.g., massive military and civilian casualties, disruption or degradation of our critical infrastructure, contamination of public health systems and foodstuffs, widespread panic, degraded response capabilities, and economic damage disruptions).

f. America’s critical infrastructure encompasses a number of interrelated sectors. Our agriculture, food mineral, and water resources, along with the public health and emergency services sectors, provide the essential 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 capabilities to help safeguard our population from external threats. 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, 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 United States 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.

g. Today, only a few countries possess the capability to perform a conventional military strike on our homeland, but given the emergence of hostile non-state entities actors, the proliferation of WMD, and asymmetric approaches to conflict, defending the homeland has become more complex. Protection of defense critical infrastructure (DCI) (i.e., our power projection platforms and command, control, communications, computers and intelligence (C4I) systems), and support to other agencies in protecting or mitigating the consequences of attacks on national critical infrastructure (NCI/KA) remains an essential task for the Armed Forces of the United States (See Figure I-5).

h. There is a continued persistent threat to our national borders posed by the influx of illegal immigrants, drugs and other smuggling contraband. This poses a unique serious threat to the nation and requires the combined efforts of conventional law enforcement personnel and, in some cases extraordinary circumstances, assistance from military sources to secure our borders and conduct counterdrug operations. Presidential Decision Directive 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 a National Special Security Event (NSSE), the Secret Service (SS) assumes the role of lead agency for the design and implementation of the operational security plan.
3. Global Security in Depth

**DOD contributes to HS through HD and CS. DOD’s HS responsibilities are global in nature and are conducted in depth beginning at the source of the threat.**

**Focusing on the source of the threat means that many missions are conducted overseas.** This approach encompasses the present strategy of deterrence, which encompasses actions such as certain overwhelming retaliation, preemption through a neutralizing first strike and seamless defenses that render any attack as futile. In addition, it must also emphasize the critical importance of mitigating the consequences of an attack if they at least are partially successful. **The geographical context of HS responsibilities entails: forward regions, approaches, and the homeland.**

- **The Forward Regions -- media outside the homeland (land, air, sea, space, and information).** In the forward regions, the objective is to deter and detect 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 attacks and defenses 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 control, and air and maritime interdiction.
Chapter I

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 – 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. Examples of operations conducted in the homeland region include air, land and maritime defenses. In addition, DOD may be required within this region to assist civil authorities in managing the consequences of attacks that have already occurred.

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.
34. Department of Defense Homeland Security Objectives

HLD and CS mission areas provide the overarching joint force approach to achieving the national military objective of securing the homeland. Specific roles that are essential in our efforts to secure the homeland include:

(1) Protecting the territorial sovereignty, domestic population and critical infrastructure of the United States.

(2) Support civilian authorities for domestic emergencies, law enforcement, the protection of national critical infrastructure and other activities as directed.

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 our efforts to secure the homeland include:

(a) Ongoing missions abroad to reduce the threat of terrorist attacks against the US.

(b) Protecting the territorial sovereignty, domestic population and defense critical infrastructure of the US.

(c) Supporting civilian authorities for law enforcement, response to domestic emergencies, protection of NCI/KA and other activities as directed; and

(d) Ensuring that emergency preparedness resources and procedures are in place in order to support the SecDef or other agencies that may require assistance.


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

b. DOD “prepares and responds” when conducting both homeland defense HD and civil support CS. DOD primarily focuses on “deters, preempts and defends” primarily when they conduct homeland defense HD missions.

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

(2) Detect. In order to effectively ensure the security and defense of the homeland, early detection of threats is essential. Detection is a national effort, which
involves common operational picture (COP) and the sharing and fusing of intelligence and information through a network of federal, state, and local agencies.

(23) Deter. An effective deterrence prevents adversaries, both state sponsored and non-state actors, from attacking the US or its interests by creating fear of the consequences of their action. Deterrence can be achieved by being so prepared for the attack that no advantage would be gained by an adversary. Deterrence is also a state of mind created by the existence of a credible and unacceptable counteraction and that is directed at potential adversaries planning attacks on the homeland.

(34) Preempt. Preemption may include proactive measures by the US in the form of a show of force; strategic positioning of military forces, or even offensive actions based on evidence that an enemy attack is imminent. Preemptive measures may prevent and or neutralize a threat or minimize the consequences of a hostile act. It may also prevent a situation from escalating into a more dangerous situation. Preemption measures also exist in the form of protecting our homeland and borders against illegal drugs and immigration. Preemption consists of proactive measures taken by the US to prevent or neutralize either a perceived or imminent attack. Preemption may include offensive actions, such as air strikes, maritime interception or direct action. In addition, intelligence gathering efforts and investigative measures may also preempt an attack. Preemption measures also exist in the form of supporting efforts to protect our homeland and borders against illegal drugs and immigration.

(45) Defend. Missions Activities associated with the HLD mission area entail the protection of the nation’s sovereignty. They orient on active and passive defense measures that are mutually supporting and
can be employed before an anticipated attack are especially beneficial. Actions to defend the homeland should contribute towards the goal of rendering hostile attacks ineffective.

(56) Respond. Response, as it relates to HLS activities, spans both homeland defense HD and civil support CS mission areas. For HLD, responding is the ability of the joint force to rapidly repel an attacker or respond to defeat an attack. DOD also provides discreet resources in the form of intelligence or investigative efforts. Military responses to assist civil authorities \textit{in the CS role, it} is the ability to rapidly and effectively assist other lead federal agencies (LFAs) in mitigating managing the consequences of disasters and catastrophes, including natural, manmade, or terrorist incidents.

c. The DOD Homeland Security Operational Framework. The overarching operational framework for DOD HLS consists of two mission areas – homeland defense HD and civil support CS. These mission areas contain a number of unique missions and functions and many activities can overlap. Synchronization and integration of selected HLD and CS missions, supporting operations and enabling activities and functions may be required and prove essential. For example, antiterrorism (AT) and force protection (FP) activities are applicable for both HD and CS. measures for both HLD and CS are of constant concern. Actions taken to prevent or mitigate hostile actions against DOD personnel (to include family members), resources, facilities, and critical information conserve the force's operational potential so it can be applied at the decisive time and place for both mission areas.

Mission areas and missions for DOD homeland security are depicted in Figure I-6 below.

---

**HOMELAND SECURITY OPERATIONAL FRAMEWORK**

**Mission Areas**
- Homeland Defense
- Civil Support

**Missions**
- Air Defense
- Land Defense
- Maritime Defense
- Military Assistance to Civil Authorities
- Military Support to Civilian Law Enforcement Agencies
- Military Support for Civil Disturbance
- Military Support for Civil Authorities

**Figure I-6. Homeland Security Operational Framework**
d. An integral part of the HLD 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 possible threats from natural disasters through to acts of terrorism. COOP planning goals normally include: 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 situations. 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, Continuity of Operations (COOP) Policy and Planning, and Chairman, Joint Chiefs of Staff (CJCS) Operation Order 3-0.

Mission areas, missions and functions of DOD homeland security operations are depicted in Figure I-7 below.

e. Within the HLD mission area, there are three missions: air and missile defense, land defense, and maritime defense. Although these missions are described in the context of the defense, HLD missions include offensive actions (preemptive as well as defensive intervention activities to deter, disrupt and destroy adversary capabilities at their source). Primary functions—Supporting operations and enabling activities associated with HLD missions may include: Defense critical infrastructure protection (DCIP) when directed, anti-terrorism AT and force protection FP, space operations, ballistic missile defense and information operations (IO)—See Chapter.

Employment of military forces within the US typically falls under the broad mission of military assistance to civil authorities
f. Employment of military forces within the US, its territories, and possessions provided under the auspices of civil support CS, typically falls under the broad category—mission of military assistance to civil authorities (MACA). MACA operations consist of three subordinate missions. They may overlap and DOD may provide support to them simultaneously, depending on the circumstances of the incident. They are: military assistance for civil disturbance (MACDIS), military support to civil authorities (MSCA), and military assistance—support to civil law enforcement agencies (MSCLEA). Military activities and operations associated with CS missions include, but are not limited to domestic chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) crisis and consequence management (CM), counterdrug operations, maritime security, NSSE support activities, disaster responses, border security, AT activities, intelligence sharing, EP activities, and IO. Some functions associated with CS missions include but are not limited to: national critical infrastructure protection (NCIP), domestic CBRNE consequence management, non-CBRNE disaster response, counterdrug operations, illegal immigration, national special security event support activities, and riots, insurrection, and unlawful obstruction or assembly.

g. Within the operational framework of homeland security, commanders may face situations during which they will be required to provide an immediate response to an incident. Immediate response is an authorized action taken by a military commander or by responsible officials or other DOD agencies while providing support to civil authorities to prevent human suffering, save lives, or mitigate extensive property damage. In certain circumstances, military commanders or responsible officials in other DOD agencies may be faced with situations that will require them to provide immediate response to civil authorities in order to prevent human suffering, save lives, or mitigate extensive 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 of officials acting under immediate response authority may take necessary action to respond, but must advise the DOD Executive Secretary (EXECSEC) of Defense through command channels by the most expeditious means available and seek approval or additional authorizations. The EXECSEC will notify SecDef, CJCS, and any other appropriate officials. The military will begin disengagement from emergency response activity as soon as practical.

h. 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) assistance to
civil authorities will involve a unique size and mix of forces. Specialized military capabilities are deployed as required. Regardless of the mix of forces and equipment, or whether the operation is associated with HD or CS, logistics operations will be required to deploy, sustain, reconstitute, and redeploy forces. These operations will require early and integrated planning among the services, sustaining organizations, combat support agencies and other federal agencies as required.

i. **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.

**Legal and Policy Environment Considerations**

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

---

![Homeland Security Campaign Model](image-url)

*Figure I-7. Homeland Security Campaign Model.*
Introduction

I-17

a. Basic Principles. The nation was founded on the principles of freedom and domestic tranquility. The Constitution provides the fundamental justification for homeland security 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. The President and Congress are key actors. These directives, policy documents, and laws provide the fundamental basis for the development of subordinate and implementing guidance by federal and state agencies.

b. Key Executive and Legislative Guidance. Presidential decision directives (PDDs) and executive orders (EOs) are the predominate means by which the President issues guidance. Prior to and after September 11, 2001, there have been a number of key documents issued by the national leadership impacting on the defense of the homeland. A list of key documents that provide guidance for the HS mission are included in Appendix A, Key Homeland Security Legal and Policy Documents. Key among these include:

Decision Directive 63 provides guidance for protecting our critical infrastructure. Executive Order 13231 extended this guidance to our key information systems.


(3) Robert T. Stafford Disaster Relief and Emergency Assistance Act, which sets the policy of the Federal Government to provide an orderly and continuing means of supplemental assistance to State and local governments. It is the primary legal authority for Federal participation in domestic disaster relief.

(4) A number of strategy documents have also been issued ranging from combating terrorism to the protection of critical infrastructure, which addresses both physical, and cyber asset protection measures.

(5) The Posse Comitatus Act (PCA) (18 USC 1385) is a key document governing DOD activities in relation to dealing with civilian authorities.

(6) Title 10 and Title 32, United States Code (USC) provides guidance to active forces and the National Guard for the conduct of homeland security operations.

c. Key Department of Defense Guidance

(1) Implications. Specific authority for HLS missions are contained in Federal and state law and policy documents. These documents form the basis for the development of DOD guidelines. DOD guidelines are promulgated in a variety of publications that include national strategy documents, planning guidance, and DOD directives. These policy documents are consistent with and complimentary to the Federal statutes and guidelines discussed earlier in this chapter. DOD Directives DODDs specifically address missions for homeland defense HD and civil support CS operations. A list of key DOD guidance is provided in Appendix A.

(2) Key DOD Guidance. There are a number of key DOD documents that will aid planners and operators in their understanding of the relationship of the DOD, Federal agencies and civil authorities. Strategy documents include the National Security Strategy (NSS) and The National Military Strategy (NMS). The NSS provides overarching guidance to the Department of Defense while the NMS interprets that and other guidance to the Nation’s Armed Forces. The Unified Command Plan provides guidance to combatant commanders, establishes missions and responsibilities, and delineates general geographic areas of responsibility. Other documents such as the Defense Planning Guidance and the Contingency Planning Guidance provide DOD planning and programming guidance for HLS activities. The primary sources for detailed guidance for DOD are Department of Defense directives (DODDs) and Chairman of the Joint Chiefs of Staff instructions (CJCSIs). Key documents identifying roles and missions include: DODD 2000.12, DOD Antiterrorism/Force Protection (AT/FP) Program; DODD 3025.15
Military Assistance to Civil Authorities; DODD 3025.1, Military Support to Civil Authorities and DODD 3025.12, Military Assistance for Civil Disturbance. These directives govern DOD military assistance to civil authorities, including support in connection with incidents involving an act or threat of terrorism. Key CJCSIs include: CJCSI 3110.16, Military Capabilities, Assets, and Units for Chemical, Biological, Radiological, Nuclear, and High Yield Explosive Consequence Management Operations; 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 and CJCSI 3125.01, Military Assistance to Domestic Consequence Management Operations in Response to Chemical, Biological, Radiological, Nuclear, or High-Yield Explosive Situation. For a detailed discussion of these and other key documents, see Appendix A.

(3d) Other Key Areas Special Considerations. Functional areas impacting the Homeland Security mission are numerous. The following discussion identifies provides general guidelines for three two areas that have unique applications when employed in an HLS operation. They also have specific legal implications of which commanders should be aware. The following provides general guidelines for intelligence, religious, and psychological operations activities in support of HLS mission areas.

(a) Intelligence Operations. Military intelligence (MI)-collection is limited in organizations have a limited role during civil support CS operations, the role of intelligence sharing and analysis is of key importance, other than civil disturbance operations—The primary focus of service intelligence units is to collect foreign intelligence (FI) and counterintelligence (CI), neither of which is typically present in a domestic support operation. To the extent that MI—military intelligence units are authorized to collect FI or CI—intelligence within the US, they may do so only in coordination with the Federal Bureau of Investigation (FBI), which has primary responsibility for 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: Executive Order (EO) 12333, United States Intelligence Activities, lays out the goals and direction of the national intelligence effort, and describes the roles and responsibilities of the different elements of the US intelligence community; Deputy Secretary of Defense Memo, Collecting, Reporting, and Analysis of Terrorist Threat to DOD Within the United States, 2 May 2003; DOD Directives 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.”

(b) Religious Operations. When crisis management or consequence management events occur within the United States or its territories, military chaplains will deploy to provide religious support (e.g., worship services, counseling, critical
incident stress management, visitation, devotions, prayers, rites, sacraments, etc.) for DOD personnel. The lead federal agency (LFA) through the federal coordinating officer (FCO) and/or the defense coordinating officer (DCO) normally will initiate requests for military chaplains. Although the Stafford Act and the Establishment Clause prohibit government sponsorship of religion, precluding military chaplains from providing religious support to civilian disaster victims, an exception to this policy may be permitted under extreme conditions. Accordingly, military chaplains may provide non-secular support to civilian disaster victims during emergency operations. Such provision will be limited to the designated, cordoned disaster control area and/or quarantine area. The duration of military chaplain ministry to civilian victims within the restricted, cordoned control area will cease with the termination of emergency operations. Moreover, the primary focus of military chaplain ministry will remain DOD personnel. A second exception to the Stafford Act and the Establishment Clause may occur if military chaplains with secular counseling expertise are asked by the LFA to provide secular counseling to civilian disaster victims. Under all circumstances, military chaplain ministry to civilian disaster victims will be initiated at the request of the LFA and coordinated through the FCO and/or the DCO. For joint guidance on religious support for Joint Operations, see JP 1-05, Religious Support for Joint Operations.

Psychological Operations. US law prohibits psychological operations (PSYOP) units from targeting US citizens. However, these assets can be used to help disseminate critical information to the civilian population. PSYOP unit personnel and equipment assets 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
AND CONSIDERATIONS

"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 through two distinct branches of the chain of command. One branch runs from the President, through the Secretary of Defense (SecDef), to the 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 the SecDef to the Secretaries of the Military Departments. The Military Departments, organized separately, operate under the authority, direction and control of the SecDef. The Secretaries of the Military Departments exercise authority through their respective Service Chiefs over their forces not assigned to the combatant commanders.

b. (1) The Combatant commanders of combatant commands exercise combatant command (command authority) of assigned forces within their respective area of responsibility (AOR) 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 respective geographic combatant command area of responsibility AORs). Combatant commanders prescribe the chain of command within their combatant commands and designate the appropriate command authority to be exercised by subordinate commanders. Command authority-relationship options include combatant command (command authority) (COCOM), operational control (OPCON), tactical control, and support. This branch is separate and distinct from the branch of the chain of command that exists within a combatant command. For detailed discussion of command relationships, see JP 0-2, Unified Action Armed Forces, Unified Action Armed Forces.

(2) 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.

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

(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 homeland defense-HD mission area, DOD conducts operations such as air, missile, land and maritime defenses and applies executes DCI defense critical infrastructure protection, force protection-FP measures and ballistic missile defenses and information operations IO commensurate with mission requirements in varying degrees for all.

(2) Civil Support

When conducting CS missions, DOD will be in support of another Lead Federal Agency (LFA). The domestic operating environment for military CS presents unique challenges to the joint force commander. It is imperative that commanders and staffs at all levels understand the relationships, both statutory and operationally, among all federal agencies involved in the operation. Moreover, it is equally important to understand DOD’s role in supporting these other federal agencies. The Department of Defense DOD will provide military assistance to the lead federal agency (LFA) and/or the concept-operation plan in concept format (CONPLAN) to primary agencies upon request by the appropriate authority and approval by the Secretary of Defense SecDef. There are various national level plans, such as the Initial National Response Plan (INRP) / Federal Response Plan (FRP), which detail the roles and missions of various federal departments and agencies in the event of a
domestic crisis. [Note: the provisions of the Federal Response Plan FRP continue to provide guidance for all activities not specifically subsumed in the INRP but will eventually be integrated into the National Response Plan (NRP).]

c-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, critical infrastructure protection, or other events, DOD could be asked to provide capabilities that other agencies do not possess or that have been exhausted or overwhelmed. In temporary non-emergency circumstances, DOD supports civil authorities where other agencies have the lead—such as providing security at a special event (e.g., US Olympics) or assisting other Federal agencies to develop capabilities to detect nuclear, chemical and biological threats.

2. Command and Control Relationships and Responsibilities

a. The President and the 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, and / 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 the strategic objectives outside the homeland may also be required
to execute HLS-HD missions within the homeland. Guidelines for command and control (C2), as depicted in JP 0-2 are equally applicable to HLS operations.

c. For DOD responses in support of another LFA the military conducts support operations in conjunction with the FRP. The United States Army Corps of Engineers (USACE) is the primary agency for public works and engineering and has supporting responsibilities for the other 12 emergency support functions (ESFs).

d. Under certain circumstances, military commanders are allowed to take necessary action under immediate response authority. 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. Under these circumstances, support elements must advise the DOD EXECSEC through command channels by the most expeditious means available and seek approval or additional authorizations. The EXECSEC will notify SecDef, the Chairman of the Joint Chiefs of Staff (CJCS), and any other appropriate officials through their chain of command must notify the action agent as soon as possible of support provided.

e. The principal and supporting DOD participants involved in the execution of HLS-HD or CS-missions areas are may include: the 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 Reserve Affairs [ASD(RA)], Chairman of the Joint Chiefs of Staff (CJCS), Commander, North American Air Defense Command (CDR NORAD), Commander, US Northern Command (USNORTHCOM), Commander, USPACOM 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), Reserve Component Forces and the Services. Reserve component forces and the US Coast Guard (USCG) are included in this grouping when under Title 10 status— and the US Coast Guard (USCG).

1. (1) Secretary of Defense. The SecDef has overall authority for the Department of Defense (DOD) and is the President’s principal advisor on military matters concerning HLS. Some DOD HLS missions overlap between HLD and CS. For example, critical infrastructure protection has both national and defense aspects. Authority for the conduct and execution of the HLD mission resides with the SecDef. For civil support missions, the SecDef retains approval authority for the use of forces, personnel, units, and equipment. (Note: Units, personnel, and equipment may be moved from military installation to military installation without SecDef approval. For operational testing and evaluation, Services may move units, personnel, and equipment between military installations without SecDef approval.) The SecDef has the primary responsibility within the DOD to provide the overall policy and oversight for CS in the event of a domestic incident.

2. (2) Assistant Secretary of Defense for Homeland Defense. The Office of the Assistant Secretary of Defense for Homeland Defense (ASD(HD)) is established within the office of the Under Secretary of Defense for Policy. The ASD(HD) provides the overall direction and supervision for policy, program planning and execution, and allocation of DOD resources for homeland defense and civil support. ASD(HD) is responsible for the overall supervision of all DOD HD activities. He has been delegated the duties and authorities associated with DOD Executive Agent assignments for MSCA and MACDIS. ASD(HD) ensures internal coordination of DOD policy direction, assists the Secretary SecDef in providing guidance, through the CJCS, to the combatant commanders for HLD missions and military activities in support to civil authorities MACA missions. It also provides conducts coordination with the Office of Homeland Security (DHS). Figure II-2 shows the organizational structure of the Office of the Assistant Secretary of Defense for Homeland Defense (ASD(HD)).

The principal duty of the ASD(HD) is to provide overall supervision of homeland defense-HD and CS-activities and civil support within DOD. In that role, the ASD(HD) responsibilities include:

(a) Developing strategic planning guidance for DOD’s role in HLS.

(b) Developing and updating force employment policy, guidance, and oversight.

(c) Overseeing DOD activities that provide MACA in domestic emergencies in accordance with existing national level emergency response plans and
approved memoranda of understanding to support civil authorities in emergencies in accordance with the Federal Response Plan.

(d) Providing DOD support, as appropriate, to assist in developing capacities and capabilities of civilian agencies requisite to conduct homeland security missions.

(e) When directed, serve as the SecDef’s executive agent for homeland defense and serve as directed with the SecDef, CJCS and the Joint Staff for HLS mission areas. Serving as the DOD domestic crisis manager focusing on coordination and integration of DOD domestic crisis activities with other departments and agencies and the combatant commanders. Exceptions include those activities requiring the use of special operations forces.

(f) Assuming responsibility for the Defense Critical Infrastructure Program (DCIP), domestic AT and FP, HD interagency coordination, HD technology transfer, NSSEs and COOP / COG.
(3) Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict. ASD(SO/LIC) provides civilian oversight for combating terrorism. This oversight includes direction for management and execution and supervision for of policy, program planning, and allocation and the use of resources for the DOD. ASD(SO/LIC) also represents the SecDef on combating terrorism matters, outside the DOD.

(4) 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 HLS response efforts. In coordination with ASD-(HD), the Joint Staff, the Services, and the National Guard Bureau (NGB), ASD(RA) ensures appropriate Reserve and National Guard NG forces are integrated into HLS response efforts.

(5) Chairman of the Joint Chiefs of Staff. The CJCS has numerous responsibilities relating to HLS. These include advising the President and the SecDef on operational policies, responsibilities, and programs; assisting the SecDef in implementing operational responses to threats or an acts of terrorism; and translating SecDef guidance into operational orders to provide assistance to the LFA. The CJCS ensures that HLD and CS plans and operations are compatible with other military plans. CJCS also assists combatant commanders in meeting their operational requirements for executing HLD missions and for providing CS that has been approved by the SecDef. In the CS area, the CJCS serves as the principal military advisor to the SecDef and the President in preparing for and responding to a CBRNE situations, and ensures that military planning is accomplished to support the lead agency—LFA for crisis management (CrM) and consequence management CM, and provides strategic guidance to the combatant commanders for the conduct of counterdrug operations.

(6) Commander, North American Air Defense Command (NORAD). NORAD is a bi-national command that conducts air defense for North America in accordance with the NORAD Agreement. CDRNORAD, By international agreement (The NORAD Agreement and Terms of Reference, and the Canadian/US Basic Security Document 100/35), CDRNORAD leads a bi-national command composed of Canadian and US forces responsible for aerospace control and aerospace warning for North America. NORAD’s relationship with USNORTHCOM is unique in that while they have separate missions defined by separate sources, a majority of USNORTHCOM’s AOR and NORAD’s operational area overlap. NORAD and USNORTHCOM are two separate commands. Neither command 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.

(67) Commander, US Northern Command. In accordance with US law CDRUSNORTHCOM has specific the responsibilities for homeland defense HD and for assisting civil authorities. Its 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 **Secretary of Defense SecDef**, provide military assistance to civil authorities including consequence management CM operations. CDR USNORTHCOM embodies the principles of unity of effort and unity of command as the single, responsible, designated DOD agency commander for overall command and control of DOD support to civil authorities within the USNORTHCOM AOR. CDR USNORTHCOM takes all operational orders from and is responsible to the President through the Secretary of Defense SecDef.

(a) Organization and Command Relationships. Figure II-3 provides the organization and command relationships for USNORTHCOM. The command organizes, and executes its missions through assigned Service components and designated functional components under its operational control (OPCON). In providing civil support CS, the command may operate through subordinate Joint Task Forces (JTF). Forces required in support of HLD and CS missions are provided through the Request for Forces process and as directed by the Secretary of Defense SecDef via Execute Orders.

![US Northern Command Organization and Command Relationships](image-url)
(b) CDRUSNORTHCOM is responsible for conducting HLD operations within the air, land, and maritime domains for its AOR, the 48 contiguous states, District of Columbia, Alaska, Canada, and all approaches to North America. CDRUSNORTHCOM exercises responsibilities for the air defense of North America through the North American Aerospace Defense Command (NORAD) conducts aerospace warning and aerospace control missions for North America. For all other areas of the AOR, CDRUSNORTHCOM exercises air defense responsibilities through the USNORTHCOM/J3. Other 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 continental United States or Alaska, will be accomplished through CDRUSNORTHCOM. When directed by the President, CDRUSNORTHCOM is responsible for conducting combat operations within the homeland utilizing forces to deter, prevent and defeat an incursion of sovereign territory. Within the designated AOR, CDRUSNORTHCOM is the supported commander for HLD missions, specifically air ballistic missile, land, and maritime defenses and protection of designated DCI.

(c) Within the designated AOR, CDRUSNORTHCOM is the DOD principal planning agent and the supported commander for the HD and CS mission areas, to include consequence management operations, support to law enforcement, and CIP. The command receives requests for military assistance in support of CS in accordance with current Department of Defense directives DODD.
Chapter II

1. Standing Joint Force Headquarters – North (SJFHQ-N). A SJFHQ is a full-time joint, C2 element within the regional geographic combatant commander’s (RCC) staff that has a daily focus on warfighting readiness and is a fully integrated participant in the RCC-commander’s staff’s planning (deliberate and crisis), and operations. It provides the RCC-commander with a trained and equipped standing, joint C2 capability specifically organized to conduct planning and develop enhanced situational understanding within an RCC-commander-designated focus area. SJFHQ-N, when directed by CDRUSNORTHCOM, will deploy to enable the rapid stand-up of establish a joint task force (JTF) MACA headquarters for large-scale MACA missions.

2. Standing Joint Task Force – Civil Support (SJTF-CS). SJTF-CS plans and integrates DOD support to the designated Lead Federal Agency LFA for domestic CBRNE consequence management CM operations. When directed by SecDef, CDRUSNORTHCOM deploys; SJTF-CS deploys to CBRNE incident sites, establishes command and control C2 of designated DOD forces, and provides military assistance to civil authorities.

3. Joint Interagency Task Force – 6 (JTF-6) North (JIATF-N). In the continental United States (CONUS), JTF-6 synchronizes and integrates DOD operations, training and intelligence support to domestic law enforcement and counterdrug efforts. When directed, JTF-6 provides operational, training, and intelligence support to domestic agencies’ efforts in combating terrorism. In the future JTF-6 will evolve into the Joint Interagency Task Force North (JIATF-N) and expand its focus beyond counterdrug to transnational threats along the land approaches to the homeland. JIATF-N conducts detection, monitoring, and handoff of suspected transnational threats within and along the approaches to CONUS; fuses and disseminates intelligence, contributes to the COP and coordinates counterdrug and combat support to lead federal agencies; and supports security cooperation initiatives in order to secure the homeland and enhance regional security.

4. Standing Joint Force Headquarters – National Capital Region (SJFHQ-NCR). Specific organization and mission TBD. Joint Force Headquarters-National Capital Region plans, coordinates, and maintains situational awareness, and as directed, employs forces for HD and military assistance to civil authorities in the National Capital Region’s operational area to safeguard the Nation’s capital.

(78) Commander, US Pacific Command. CDRUSPACOM serves as DOD principal planning agent and supported commander for military HLS activities in Hawaii, Territory of Guam, Territory of American Samoa, and Commonwealth of the Northern Mariana Islands, US administrative entities, and US territorial waters within Pacific Command. CDRUSPACOM is the supported commander within the designated AOR for HLS missions, specifically air and missile, land, and maritime defenses. CDRUSPACOM is also responsible for combating terrorism actions, force protection, and performing DCIP DCI protection functions. When directed by the President, CDRUSPACOM is responsible for conducting combat operations within the AOR to deter, prevent and defeat an incursion of sovereign territory. CDRUSPACOM is also
the DOD principal planning agent within the AOR for CS operations. Responsibilities included within the overarching military assistance to civil authorities include tasks associated with MSCA, MSCLEA and MACDIS.

(89) Commander, US Strategic Command (CDRUSSTRATCOM). The principal mission of US Strategic Command (USSTRATCOM) is to conduct full-spectrum global strike operations and coordinated space and information operations to meet both deterrent and decisive national security objectives 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, integrated missile defense, global C4ISR and specialized planning expertise to the joint warfighter.

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

1. Planning, integration and coordination of global missile defense operations and support, (air, land, maritime, and space-based). This includes the development of support for missile defense and development of desired characteristics and capabilities for global missile defense operations and supporting activities associated with missile defense.

2. Provide integrated global strike planning and C2—command and control in support to deliver rapid, extended range, precision kinetic and nonkinetic fires 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, integration and coordination of DOD information operations—IO capabilities that have a trans-regional impact or that directly support national objectives.

4. Planning, integration and coordination of intelligence, surveillance and reconnaissance in support of strategic and global operations, as directed, and implement security assistance relating to military space operations and provide military assessments as required.

5. Planning and implementation of security assistance relating to military space operations and provide assessments as required.

(b) CDRUSSTRATCOM also serves as the supporting commander to USNORTHCOM and USPACOM for homeland defense—HD and civil support—CS missions—activities within their AORs.

(910) Commander, US Special Operations Command. The CDRUSSOCOM serves as a supported or supporting commander for designated global strike operations
and selected counter terrorism activities and serves as the supporting commander to USNORTHCOM and United States Pacific Command (USPACOM) within their respective AORs when requirements exceed conventional forces capabilities and special operations forces expertise is needed. When directed by the President or the SecDef, C4DRUSSOCOM conducts special operations and provides special operations forces as required in support of the LFA during civil support operations. C4DRUSSOCOM may also provide liaison officers and other assistance to the supported combatant commanders as required.

(11) Commander, US Transportation Command—(CDRUSTRANSOCOM). CDRUSTRANSOCOM is a supporting commander to CDRUSSTRATCOM, CDRUSNORTHCOM, CDRUSPACOM, and CDRUSSOCOM 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. During HD operations, CDRUSTRANSOCOM serves as the supporting commander to USSTRATCOM for designated global strike operations and selected counter terrorism activities. CDRUSTRANSOCOM also serves as the supporting commander to USNORTHCOM and USPACOM within their respective AORs for HD and CS missions.

(12) Commander, US Joint Forces Command—(USJFCOM). CDRUSJFCOM’s role in Homeland Security HS is to provide support to other combatant commands in their role as Joint Force Provider, Joint Force Integrator, and Joint Force Trainer.

(13) Commander, US Southern Command

(a) CDRUSSOUTHCOM is a supporting commander to USNORTHCOM for HLD. Principal functions include the detection and monitoring of narcoterrorism and drug trafficking activities in source and transit zones. To assist in the defeat of narcoterrorism drug trafficking, USSOUTHCOM components conduct surveillance of air and maritime routes to the United States. USSOUTHCOM monitors illicit trafficking 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 homeland security HD and civil support CS missions areas for US territories in the Caribbean.

(14) Reserve Component (RC) Forces. National Guard NG and Reserve forces are collectively referred to as Reserve Component (RC) Forces and are integral to the
accomplishment of peacetime missions and conflict prevention. They are also an essential part of the homeland security HS operational force and consist of the US Army National Guard NG, the US Army Reserve (USAR), the US Naval Reserve (USNR), the US Marine Corps Reserve (USMCR), the US Air National Guard NG, 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 NGB is the channel of communications 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 Army and Air NG of the US.

(2) Ensuring that units and members of the Army and Air NG are trained by the states in accordance with approved programs and policies of, and guidance from the Secretaries of the Army and 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 National Guard NG primarily operates under three different C2 relationships: Federal funding and Federal control (Title 10 USC); Federal funding and State control (Title 32 USC); and State status (State funding and State control). National Guard NG adjutants generals and commanders

The National Guard responds to Civil Support incidents that require resources beyond the capabilities of local and state-level emergency response organizations.
are responsible for planning and training for both Federal and State missions.

1. The National Guard NG, when in State status, responds under the Governor’s control for HLD-CS missions in accordance with State laws. However, when National Guard NG personnel or units are federalized by order of the President under Title 10 USC, they respond under the same guidelines, legal restrictions, and C2 structures as active component military forces.

2. The National Guard 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 National Guard NG, operating under Title 32 USC or State status, is likely to be the first large-scale military responder to a WMD-CBRNE incident site or area. The WMD-CSTs mission is to deploy on short notice to an incident site in support of a local incident commander and to assess a suspected site. WMD-CSTs advise local and regional officials on the short and long term ramifications associated with the incident, based on the weapons or agents that were used, and facilitate requests for additional State and Federal assistance to save lives, prevent human suffering and mitigate greater property damage.

4c. Reserve Forces. Each of the seven reserve components is structured and operated in a manner similar to its respective active duty parent service. Unlike the Army and Air National Guard NG, 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. They When called to active duty, Reserve Forces conduct HLS missions under Title 10 guidelines exactly as their active component parent services. While on active duty, members of the USAR, USNR, USAFR, USMCR and the USCGR are subject at all times 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 Reserve Component the RC mobilization/demobilization process, see JP 4-05.1, Joint Tactics, Techniques, and Procedures for Manpower Mobilization and Demobilization Operations: Reserve Component Callup.

(15) US Coast Guard. The USCG operates under is a military service and a branch of the Armed Forces in the Department of Homeland Security DHS (Title 14, USC 1). When directed by executive order of the President or upon declaration of war by Congress, the USCG shall transfer to the Department of the Navy for operations. The Commandant USCG will report directly to the Secretary of the Navy (SECNAV) for
all matters pertaining to equipping, training and employment of the service. The SECNAV will assume those statutory duties granted to the secretary of the department to which the USCG is assigned.

(a) The Coast Guard USCG’s homeland security-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, the USCG will prepare for and, in event of attack, conduct emergency response operations. Under extraordinary circumstances that require DOD to execute traditional military missions, such as air combat patrols or maritime defense operations, the Coast Guard may serve in supported or supporting roles when conducting Title 10 military operations.

(b) The USCG is the LFA responsible for the conduct and coordination of maritime security operations carried out under civil authorities for HLS in the US maritime domain. When the USCG is serving in this role, DOD assets will normally serve in a supporting role, however C2 relationships will be tailored to the particular situation. The provisions detailed in DODD 3025.15, Military Assistance to Civil Authorities, apply for approval authority and execution procedures when military assistance is provided to civil authorities. There are situations where the USCG is a supporting agency operating in support of other Federal, State, and local civil agencies and The USCG 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 upon protocols. In its maritime law enforcement role, the 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.

(c) When elements of the USCG are assigned to DOD for execution of maritime HD missions, the USCG 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. Normally in time of war, the combatant commander
will assign USCG activities OPCON to the appropriate component commander.

3. Federal Agency Responsibilities and Considerations.

Disasters are initially and ultimately local events. Local and State authorities have primary responsibility to fund, prepare, and operate emergency services. Local resources are first to respond and last to leave the scene. Local citizens have an immediate and enduring interest. Figure II–4 illustrates this process of a bottom up response beginning at the local level. DOD is one of many federal agencies and organizations with HS responsibilities. To facilitate coordination of these various efforts 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 (NSA) of 1947. The NSA-47, as amended, established the National Security Council (NSC) to advise the President with respect to the integration of domestic, foreign, and military policies relating to national security. There are six NSC Policy coordination committees (PCCs). Two that relate closely to HLS are: “Counterterrorism and National Preparedness,” and “Proliferation, Counterproliferation, and Homeland Defense.” Homeland Security Presidential Directive (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 equities. See Homeland Security Presidential Directive-1 for more information.
b. Interagency Coordination 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 of all instruments of national power is required to ensure the successful execution of HLS missions. The challenges facing the nation are increasingly complex and will require the skills and resources of many organizations. Guidelines for interagency coordination include:

1. Achieving Unity of effort amongst a mix of Federal, State and local agencies.
2. Identifying all agencies and organizations potentially involved in the operation.
3. Identifying key elements of information that various agencies can share.
4. Establishing an interagency hierarchy and defining the objectives of the response effort.
5. Identifying appropriate resources to include C4I capabilities of each participant.
6. Defining the objectives of the response effort.
7. Defining the desired end state and exit criteria.
8. Defining courses of action for the supporting effort.
9. Identifying potential obstacles.
10. Maximizing the mission’s assets to support long-term goals.
11. Establishing interagency assessment teams.

Figure II-5 synopsizes the guidelines depicted above.

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.

c. HD and CS interagency coordination activities require detailed planning and the development of 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 missions. ASD(HD) is responsible for coordinating all HD and CS matters with other executive departments and federal agencies. ASD/HD will ensure that the evolution of DOD strategy is consistent with and fully supports the national HS effort. Figure II-5 portrays DOD HS interagency relationships.
• Define the Objectives, End State, and Transition Criteria.
• Establish a Common Frame of Reference.
• Develop Courses of Action or Options.
• Capitalize on Experience.
• Establish Responsibility.
• Plan for the Transition of Key Responsibilities, Capabilities, and Functions.
• Define the Problem in Clear and Unambiguous Terms.
• Direct All Means Toward Unity of Effort.

**Figure II-4. Guidelines for Interagency Coordination.**

**INTERAGENCY COORDINATION**

![Diagram of interagency coordination](image)

**LEGEND:**
- Policy & Reqts Coordination
- Guidance, Direction, & Tasking
- Activity Coordination

**Other DOD Agencies/Activities**
- NORTHCOM Combatant Commands
- USCG
- NIPC
- NCS
- FEMA

**Other DHS Agencies/Activities**
- FBI/JTFF
- U.S. Attorney/ATTF
- USGS
- U.S. Marshal
Command Relationship, and Interagency Responsibilities and Considerations

The Federal Response Plan (FRP). The FRP defines the responsibilities of the various Federal departments and agencies that provide Federal assistance to State and local efforts in dealing with the consequences of significant disasters. The FRP is coordinated and managed by Federal Emergency Management Agency (FEMA). This plan is the result of agreements between FEMA and the primary and supporting Federal agencies responsible for providing disaster relief support. The primary agency for resource support under this Plan is the General Services Agency. Supporting departments and agencies include: Agriculture, Commerce, Defense, Energy, Labor, Transportation, Treasury, Veterans Affairs, FEMA, National Aeronautics and Space Administration, National Communications System and the Office of Personnel Management. There are twelve Emergency Support Functions in the FRP. DOD has primary responsibility for Emergency Support Function (ESF) 3, “Public Works and Engineering” and supporting responsibilities for all ESFs (See Figure II-6 for a depiction of FRP ESFs). DOD resource support under this Plan 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. Interagency Plans. Given the complexity and extent of federal, state and local participation in domestic incident management, there are various operational federal level plans and agreements that depict the roles and responsibilities of participants in different incident management and emergency response circumstances. Documents such as the FRP, U.S. Government Interagency Domestic Terrorism Concept of Operations Plan, Federal Radiological Emergency Response Plan, Mass Migration Emergency Response Plan, and the National Oil and Hazardous Substances Pollution Contingency Plan are designed to provide guidance for responding to various domestic emergencies. The intent is to integrate these plans into an all-hazards NRP. However, at present, only an INRP has been produced. While this document will serve as a bridge between the current family of documents and the NRP, the current family of response plans remains in effect until a final NRP has been developed and approved. (See Chapter IV for more details on the INRP).

(1) The FRP is executed in response to an actual event requiring Federal assistance under a Presidential declaration of a major disaster or emergency. When a major disaster occurs (or before, for predictable events) the regional FEMA director activates a regional operations center (ROC). The ROC staff is the initial coordination organization for Federal activity. Other elements of the initial Federal response may include an emergency support team (EST) and an emergency response team (ERT). The ERT coordinates the overall Federal response and recovery activities and provides assistance and support to the affected state and local governments. The ERT is headed by a federal coordinating officer (FCO) and operates from a disaster field office (DFO). At the State level, the state coordinating officer (SCO) has roles and responsibilities similar to those of the FCO. The SCO coordinates State and local assistance efforts with those at the Federal level. The EST is an interagency group that operates from the Emergency Information and Coordination Center located at FEMA headquarters. Its role is to coordinate and support the Federal response to a specific incident.
(2) DOD may serve as a support agency to the FBI for crisis management functions, and as a support agency to FEMA for consequence management. In accordance with DOD Directive 3025.15, the Chairman Joint Chiefs of Staff CONPLAN 0500-00, and upon approval by the Secretary of Defense, DOD will provide assistance to the LFA and/or the CONPLAN primary agencies, as appropriate. DOD assistance includes threat assessment; domestic emergency support team (DEST) participation and transportation; technical advice; operational support; support for civil disturbances; custody, transportation and disposal of a WMD device; and other capabilities including mitigation of the consequences of a release. DOD has many capabilities for dealing with a WMD and combating terrorism (see Appendix __ for a list of these capabilities). These and other DOD assets may be used in responding to an incident if requested by the LFA and approved by the Secretary of Defense.

(3) In response to a catastrophe, FEMA conducts emergency operations to save lives and property by positioning emergency equipment and supplies, evacuating potential victims, providing food, water, shelter, and medical care to those in need, and by restoring critical public services. FEMA supports the long-term recovery, by rebuilding communities so individuals, businesses, and governments can function on their own and return to normal life.

d. Federal Radiological Emergency Response Plan (FRERP). The FRERP provides the federal government’s concept of operations based on specific authorities for responding to radiological emergencies and outlines Federal policies and planning considerations on which concepts of operation and the Federal agency response plans are based. The FRERP also specifies authorities and responsibilities of each Federal agency that may have a significant role in such emergencies. The FRERP covers any peacetime radiological emergency that has potential radiological consequences within the United States, its Territories, possessions, or territorial waters. The level of the Federal response depends on the specific emergency. Emergencies occurring at fixed nuclear facilities or during the transportation of radioactive materials, including nuclear weapons, fall within the scope of the Plan regardless of ownership. Agencies committing resources under this Plan do so with the understanding that the duration of the commitment will depend on the nature and extent of the emergency and the State and local resources available. State and local governments may request assistance under this Plan directly to FEMA or to other Federal agencies with whom they have preexisting arrangements or relationships.


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-5 reflects this relationship. The response to an incident within the US will entail a highly coordinated, multi-agency, local, State, and Federal response. In support of this mission the following departments and agencies depicted in Figure II-7 will provide the core Federal response.
a. Department of Justice (DOJ)/Federal Bureau of Investigation (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 these acts of terrorism that violate U.S. federal law (for a discussion of crisis management, see Chapter IV). DOJ has charged the FBI with execution of its LFA responsibilities for the management of a Federal response to terrorist threats or incidents that take place within US territory or those occurring in international waters that do not involve the flag vessel of a foreign country. The FBI will implement a Federal crisis management response as LFA, 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 FEMA. The FBI, with appropriate approval, will form and coordinate the deployment of a DEST with other agencies, when appropriate, and seek appropriate Federal support based on the nature of the situation. President’s Homeland Security Advisory Council (PHSAC). The PHSAC 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;

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 (DHS). The Homeland Security Act of 2002 established this department with five subordinate directorates, and two independent Services – the Secret Service and the Coast Guard. Figure II-8 shows the organizational structure of the Department. Each of the five subordinate directorates is discussed below.

![Department of Homeland Security Organizational Structure](image-url)
(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 unifies authority over all Federal security operations, our land and maritime borders, in territorial waters, and among transportation systems. Elements of the Customs Service, Immigration and Naturalization Service (INS) and Border Patrol Bureau of Citizenship and Immigration Services, Bureau of Immigration and Customs Enforcement, Bureau of Customs and Border Protection, the Animal and Plant Health Inspection Service of the Department of Agriculture, the Federal Protective Service, Office for Domestic Preparedness and the Transportation Security Administration are elements of this directorate and are the single government entity that manages entry into the United States. Border and Transportation Security—The Federal Protective Service is assigned the role of protecting government buildings -- a task closely related the 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. It manages critical response assets such as the Nuclear Emergency Search Team (Department of Energy) and the National Pharmaceutical Stockpile—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. The Federal Emergency Management Agency (FEMA) is the primary agency operating in support of this directorate—FEMA.

(3) The Science and Technology Directorate is the primary research and development arm of the DHLS. It organizes the scientific and technological resources of the United States to prevent or mitigate the consequences of attacks on the nation—it 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 leverages draws from multiple sources – including the Central Intelligence Agency (CIA), NSA, FBI, Immigration and Naturalization Service (INS), Drug Enforcement Administration, Department of Energy (DOE), Customs, Department of Transportation (DOT) and data gleaned from other organizations. This directorate provides the capability to identify and assess current and future threats to the homeland, map threats against current vulnerabilities, issue timely warnings, and immediately take appropriate preventive and protective action. The directorate is also responsible for evaluating 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, 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 DHS.

(6) The Secret Service is one of two agencies that transferred intact to DHS. The primary mission of the SS 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 financial and critical 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. The SS 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). DOE serves as a support agency to the FBI for technical operations and a support agency to FEMA for consequence management. DOE provides scientific and technical personnel and equipment in support of the LFA during all aspects of a WMD incident. DOE assistance can support both crisis and consequence management activities with capabilities such as threat assessment, defense emergency support team (DEST) deployment, LFA advisory requirements, technical advice, forecasted modeling predictions, and operational support to include 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 clean-up; 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 Energy 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 these acts of terrorism that violate US federal law. 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 the flag vessel of a foreign country. The FBI will implement a federal CM response as LFA, 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 FEMA.
Environmental Protection Agency (EPA). The EPA serves as a support agency to the FBI for technical operations and a support agency to FEMA for consequence management. EPA provides technical personnel and supporting equipment to the LFA during all aspects of WMD incidents. The 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. EPA assistance and advice includes threat assessment, consultation, agent identification, hazard detection and reduction, environmental monitoring; sample and forensic evidence collection/analysis; identification of contaminants; feasibility assessment and clean-up; and on-site safety, protection, prevention, decontamination, and restoration activities. The EPA and the United States Coast Guard (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. The EPA provides the pre-designated federal on-scene coordinator for inland areas while the USCG coordinates resources for the containment, removal, and disposal efforts and resources during an oil, hazardous substance, or WMD incident in coastal areas.

Department of Health and Human Services (DHHS). DHHS serves as a support agency to the FBI for technical operations and a support agency to FEMA for consequence management. 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. 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. Operational support to FEMA may include mass immunization, mass prophylaxis, mass fatality management, pharmaceutical support operations (Strategic National Pharmaceutical Stockpile), contingency medical records, patient tracking, and patient evacuation and definitive medical care provided through the National Disaster Medical System.

fg. **United States** Department of Agriculture (USDA). USDA serves as the primary support agency to FEMA for disaster relief and consequence management for firefighting and food ESFs 4 and 11. USDA manages and coordinates firefighting activities by providing personnel, equipment and supplies in support of State and local agencies involved in rural and urban 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.

gh. **General Services Administration (GSA).** GSA serves as the primary support agency to FEMA for resource support during disaster relief and consequence management operations. GSA provides emergency supplies, space, office equipment, office supplies, telecommunications (in coordination with ESF 2), contracting services, transportation services (in coordination with ESF 1), 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 and blood and blood products.

Hd. **Requests for Assistance.** Upon execution of the FRP, requests for military resource support must be accompanied by a Request for Federal Assistance, unless the DOD component is responding under its independent funding authority or the commander’s immediate response authority. (Note: The inability to immediately obtain an RFA should not preclude approved support.) USNORTHCOM, USSTRATCOM and USPACOM will perform HLD functions primarily through a coordinated military response and will be in accordance with the mission as established through military channels. Response to CS incidents is more complicated in that it has the potential to address multiple incidents. Although there are similarities among the majority of them, each possesses its own unique requirements. Requests for Federal assistance by State and local governments, as well as those from owners and operators of critical infrastructure facilities, are coordinated with the lead agency (crisis or consequence) responsible under US law for that function. In response to a terrorist threat or incident, multiple or competing requests will be managed based on priorities and objectives established by the Joint Operations Center (JOC) Command Group. State and local governments will submit requests for Federal crisis management assistance through the FBI. State governments will submit requests for Federal consequence management assistance through standard channels under the Federal Response Plan. FEMA liaisons assigned to
the DEST or JOC coordinate requests with the LFA to ensure consequence management plans and actions are consistent with overall priorities. All other requests for consequence management assistance submitted outside normal channels to the DEST or JOC will be forwarded to the regional operations center (ROC) director or the Federal coordinating officer (FCO) for action. As mandated by Presidential Decision Directive (PDD)-39, Federal agencies directed to participate in counterterrorist operations or the resolution of terrorist incidents bear the costs of their own participation, unless otherwise directed by the President. This responsibility is subject to specific statutory authorization to provide support without reimbursement. In the absence of such specific authority, the Economy Act applies, and reimbursement cannot be waived. Requests for support occur in a variety of ways, Figure II-9 provides an example of the hypothetical sequence of events and when local and federal responders may get involved given an evolving disaster.

Other examples of specific responses include:

(45) 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. FEMA has the primary responsibility for coordination of Federal assistance to State and local governments.

(2) During MACA, the DOD, in coordination with FEMA, generally supports Federal agencies that have primary emergency support function (ESF) responsibility in the FRP. This coordination is effected between the defense coordinating officer and the Federal coordinating officer (FCO) and the process remains the same for CBRNE CM. When the DOD provides military support to LEAs, DOJ is generally the LFA.

(3) In military support to incidents involving CBRNE, the DOD supports the LFA through USNORTHCOM or USPACOM. USNORTHCOM will normally respond in a lead or supporting role with its Joint Forces Task Force Civil Support (JTF-CS). USNORTHCOM will respond when the President issues a Federal emergency declaration and approves the use of DOD assets in support of the LFA.

(4) b. Specific approval authority for the use of DOD assets is designated by the SecDef. This approval authority applies in the case of sensitive support requests, threats and acts or threats 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.

(5) c. Federal agencies may request DOD support based on interagency memoranda of agreement (MOAs). For example, under an interagency memorandum of agreement (MOA), the US Navy may deploy oil containment and recovery equipment to support USCG (Department of Homeland Security 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 DOD Office of the General Counsel.
CHAPTER III
HOMELAND DEFENSE OPERATIONS

“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. Under the DOD HLD mission area, the President, exercising his constitutional authority, authorizes military action capabilities are used to counter external threats and aggression against the United States. The President’s inherent constitutional authority for HLD may also be used in cases such as a terrorist attack where normal measures are insufficient to carry out Federal functions. Supported by other agencies, DOD will take the lead in defending the US against external threats and aggression. Normally, DOD is the lead, supported by other agencies, in defending against traditional external threats/aggression (e.g., air and missile attack). However, against asymmetric, non-traditional threats, perhaps internal (e.g., terrorism), DOD would support DHS. In any case, for HD, DOD will be working in conjunction with or coordinating operations with a federal agency or department.” Consistent with laws and policy, the Services will provide joint force capabilities to support combatant command requirements against a variety of air, land, sea, space, and cyber incursions that can threaten national security. These include invasion, computer network attack, and air and missile attacks. The desired end state for joint force purposes of HLD efforts is to protect against, and/or mitigate the impact of unwanted incursions or attacks on sovereign territory, the domestic population, and defense critical infrastructure. The following goals guide the DOD regarding HLD:

   (1) Dissuading adversaries from undertaking programs or conducting actions that could pose a threat to the U.S. homeland.

   (2) Assuring defense of the homeland and denying adversary’s access to the nation’s airspace, land, and maritime approaches.

   (3) Assuring access to space and information.

   (4) Denying access to defense critical infrastructure assets.

   (4, 5) Deterring aggression and coercion by deploying forward with the capacity to swiftly defeat attacks on the homeland and imposing severe penalties for aggression on an adversary’s military capability and supporting infrastructure.

   (5, 6) Decisively defeating any adversary if deterrence fails.

   (7) Minimize the consequences of any attack or incident.
b. Operations Outside the Homeland. Outside of the United States, DOD conducts HLD by preventing and denying adversaries access to the nation’s air, land, and maritime approaches. It also includes activities that secure our freedom to operate in space and cyber space ability to access information.

c. Military Activities Within the Homeland. Operations encompass all land, airspace, and sea territory of the United States, which includes the 50 States, the District of Columbia, possessions and protectorates and includes our freedom to operate in space and cyberspace and to access information. It also includes protection of DCI assets located within the homeland.

2. Homeland Defense Operational Elements and Characteristics

a. DOD HLD missions are conducted in accordance with DOD, CJCS, Joint, Military Department and military service policy, directives, doctrine and tactics techniques and procedures. HLD activities are operationalized—conducted at the operational level through a combination offensive actions, and active and passive defenses. They are further enabled by command, control, communications, computers and intelligence (C4I) systems. Figure III-1 is a graphic depiction of the HLD characteristics, missions, operational elements and enablers.
b. HLD missions begin with thorough preparation. HLD emergency preparedness (EP) activities are undertaken to ensure DOD processes, procedures and resources are in place to support the President and Secretary of Defense - SecDef in a designated national security emergency. DOD EP responsibilities 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 efforts, joint training exercises and experimentation and development of seamless information and intelligence architectures.

c. Deterring adversaries is a key HLD objective and DOD EP efforts, coupled with offensive and defensive capabilities, may deter an adversary from threatening or attacking the homeland. Training and preparation, weapons, forces, command and control - C2 and proactive intelligence gathering are a few examples of actions and capabilities that may serve as deterrents.

d. If deterrence fails, DOD must be prepared to rapidly respond and defend against threats and aggression. Preemptive actions, although offensive in nature, are classified as a layer in DOD’s homeland defenses. DOD will only as directed by the President, may conduct preemptive /offensive HLD actions in accordance with international and domestic law, national policy, and directives. The objective of these operations is to destroy, disrupt, or neutralize weapons, launch platforms, supporting command, control, and communications, logistics and intelligence, surveillance, and reconnaissance (ISR) capabilities before they are employed by an adversary. Air, land, sea, space and special operations forces may conduct offensive actions. Examples of operations include global strikes. Global strikes are rapidly planed, limited-duration, extended-range precision attacks that are conducted to achieve strategic objectives. Global Strikes may be executed against highly valued adversary assets using both kinetic and non-kinetic methods. Global Strike 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, direction action, space negation denial and computer network attacks.

e. Primary defensive actions associated with HLD missions orient on include active and passive defense measures. The objective of HLD active defenses is to defeat threats that are already deployed or enroute to the target. Active defenses are layered and deployed in depth and are designed to destroy, nullify, or reduce the effectiveness of attacks on our sovereign territory, domestic population and critical assets using both kinetic and non-kinetic weapons capabilities. Active defenses employ air, land, sea, space, and special operations forces. Defenses may also include active electronic warfare and offensive information operation - IO capabilities to disrupt adversary information systems. The objective of HLD passive defenses is to mitigate /minimize the consequences of attacks that may be successful/reduce the probability of and minimize the damage caused by hostile actions. Passive defenses include force protection - FP measures and actions and critical infrastructure risk mitigation actions to
reduce targeting effectiveness. They are normally developed and executed throughout the defending force from the highest to the lowest levels. Passive defense capabilities include selected AT activities, deception, mobility, dispersion, systems hardening, and protective construction, strategic, operational, and tactical warning, and recovery and reconstitution efforts.

f. Command, control, communications, computers and intelligence (C4I) systems enable all homeland defense (HD) offensive and defensive efforts. C4I systems enable centralized planning and the coordinated and mutually supporting employment of forces and assets. A common operational picture (COP) facilitates decentralized execution in rapidly changing operational environments. Intelligence and information systems must be shared among appropriate agencies to include law enforcement when building the COP. C4I systems and architectures also provide commanders with the capabilities necessary to plan missions, control and direct forces and coordinate and execute operations. Effective C4I systems for air and missile, 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, data sources and communications systems. An example of a critical C4I asset is the Cheyenne Mountain Operations Center (CMOC). NORAD's warning and assessment capabilities used to support the integrated tactical warning/attack assessment (ITW/AA) process. Within NORAD, the CMOC, the commands involved in homeland air and missile defenses (USNORTHCOM, USELEMM, NORAD, USPACOM, and USSTRATCOM) share selected C4I systems and architecture, which enables effective coordination, synchronization, and seamless defenses.

3. Homeland Defense Missions

a. Joint force HD activities encompass orient on three broad missions: air and missile defense, land defense, and maritime defense. When directed by the President and the Secretary of Defense (SecDef), DoD conducts HD missions in defense of our population, sovereign territory and critical assets. 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 homeland air and missile, land, and maritime defenses. NORAD is charged with aerospace warning and aerospace control for North America. Aerospace warning includes the monitoring of man-made objects in space, and the detection, validation, and warning of attack against North America whether by aircraft, missiles, or space vehicles, utilizing mutual support arrangements with other commands. Aerospace control includes providing surveillance and control of Canadian and United States airspace. NORAD's commander is also CDRUSNORTHCOM.

b. Selected HD missions and functions will likely require extensive integration and synchronization and may also overlap and occur simultaneously. In addition, HD
military responses may transition to one or more types of civil support. For example, attacks on the homeland intended to destroy national critical infrastructure could cause mass evacuation and relocation of civilians in addition to extensive casualties. In this instance, while executing offensive operations and active defenses 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 is a graphic depiction of the three HD missions (air defense, land defense and maritime defense). The following outlines and describes the missions associated with homeland defense:

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

1. Air and missile defense includes all measures of homeland defense taken to deter, detect, defeat or nullify hostile air and missile threats against the US homeland – territory, domestic population and infrastructure. Air and missile defenses consist of two missions that must operate in unison for maximum effectiveness: air defense, which is designed to destroy, nullify, or reduce the effectiveness of attacking enemy aircraft, both manned and unmanned and cruise missiles; and ballistic missile defense, which defeats long-range ground and sea-launched ballistic missile threats. No single action is capable of providing complete protection from a coordinated air or missile attack and a combination of offensive operations and active and passive defense measures will likely be required.

2. Land defenses include all measures of HD taken under extraordinary circumstances to deter, and if necessary, defeat land threats when the President directs or
SecDef orders. Land defenses include all measures of homeland defense taken to deter, detect defeat or nullify hostile land threats against the US homeland—territory, domestic population and infrastructure. 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 operations and establish active and passive defenses in depth and along our borders to counter a host of conventional and asymmetric threats.

(3) Maritime defenses involve all measures of homeland defense—HD taken to deter, detect, 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 operations and active and passive defenses in depth to counter conventional or asymmetric maritime attacks within US territorial waters. For more information concerning homeland defense operations see JP 3-26.1, Joint Doctrine for Homeland Defense. When published detailed information concerning HD—operations will be contained in JP 3-26.1, Joint Doctrine for Homeland Defense.

4. Common Functions—Supporting Operations and Enabling Activities

a. HLD common functions—supporting operations and enabling activities include consist of defense critical infrastructure protection (DCIP), space operations, anti-terrorism (AT) and force protection (FP) (AT/FP) activities, ballistic missile defense, and information operations (IO). Supporting missions and activities These functions should be considered in the planning and execution of all aspects of HLD air and missile, land and maritime defenses and are generally applied as series of overlapping protection and defensive measures. HLD supporting missions and activities functions often overlap with one another and specific tasks may be closely related. For example, when performing activities associated with protecting defense critical infrastructure (a key DOD installation), planners must also consider anti-terrorism—AT and force protection—FP measures to protect individual service members or specific facilities and equipment (physical assets). Continued operation of information systems deemed vital to installation C2 (cyber-computer network defenses and information assurance activities) will also be required. Figure III-2 is a graphic depiction of the three HLD missions (air and missile defense, land defense and maritime defense) and the supporting common functions (DCIP, AT/FP and IO).

b. The following describes the HLD supporting missions and activities identified above common function—general responsibilities and how they may be applied across the HLD missions area.

(1) Critical Infrastructure Protection (CIP). CIP activities associated with defense critical infrastructure consist of the identification, assessment and security enhancement of assets essential to mobilize, deploy and sustain DOD military operations. DCI generally consists of physical (installations, and 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 effort that provides a comprehensive process for understanding and protecting selected infrastructure assets that are critical to national security during peace, crisis, and war. Figure III-3 graphically portrays how DCIP is organized within DOD. DCIP addresses the relationship between combatant commanders’ capabilities, systems and functions, their supporting critical assets, and force readiness. DCIP involves identifying, visualizing, assessing, protecting, monitoring, and assuring the reliability and availability of mission-critical infrastructures essential to the execution of the NMS. The DCIP Program also addresses the operational decision support necessary for combatant commanders from all defense components to achieve their mission objectives despite the degradation or absence of these infrastructures. For more information concerning CIP and the Defense Critical Infrastructure Program see DODD 3020.XX.

(1) Defense Critical Infrastructure Protection Activities. Defense critical infrastructure protection (DCIP) consists of the identification, assessment and security enhancement of physical and cyber assets essential to mobilize, deploy and sustain DOD military operations. DCIP activities are designed to identify and protect infrastructures that are deemed critical to DOD force readiness and operations in peace, crisis and war.
DCIP activities also contribute to mitigating the consequences of any losses or disruption and facilitate timely restoration and recovery. DOD will serve as the lead federal agency to prepare for, respond to, and defend against adversary attacks on defense critical infrastructure and assets. DCIP activities are generally managed under the critical asset assurance program (CAAP). Critical asset assurance is a comprehensive process of identifying assets deemed critical to DOD. Though CAAP potential threats are assessed, potential actions are then identified to restore those assets if lost, damaged, corrupted or compromised. CAAP also facilitates the identification of options and recommendations for conducting activities to protect, mitigate and improve the availability of designated critical assets.

(a) DOD serves as the lead federal agency to prepare for, respond to, and defend against adversary attacks on defense critical infrastructure. The ASD(HD) acts as the principal staff assistant and civilian advisor to SecDef on CIP activities and provides oversight authority for DOD CIP policy implementation and CIP resource and budget planning. Defense critical infrastructure (DCI) generally consists of physical, cyber, information, and power projection capabilities and assets. Protection measures for all DCI should be integrated with the planning, coordination and synchronization that are required for every Service installation, base, ship unit and port. Examples of DCI include military C4I networks and centers, designated critical logistics assets and distribution capabilities, selected strategic mobilization sites, and key defense aerial and sea ports of embarkation. Additional examples of DCI assets that DOD will likely be tasked to protect and defend are shown in Figure III-3. It should be noted that complete protection of just one asset may require the application of a range of DCIP measures.

(b) Respective combatant commanders conducting HLD missions are responsible for establishing critical infrastructure protection (CIP) programs that conform to DOD requirements and policy. As shown in Figure III-3 DCI is broken down into ten sectors. Each sector has a designated lead responsible for protection activities. Combatant commanders should coordinate with the Military Departments and appropriate Defense agencies and sector leads to identify, prioritize, and assess vulnerabilities of all of those critical assets and non-DOD infrastructure dependencies necessary for the successful execution of present and projected military operations within their AORs. DOD components are also responsible for establishing CIP programs that are in accordance with DOD requirements and policy. They 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 projection of US interests at home. Components also address CIP issues at the installation level.

(c) Defense power projection capabilities primarily consist of CONUS-based DOD facilities—assets, infrastructure, and systems that enable the joint force DOD to project military power globally. Examples include designated strategic military bases, ports of embarkation (POEs)/ports of debarkation (PODs), mobilization centers, staging and storage areas, rail and trucking transportation centers, etc. Defense of these facilities is normally in coordination with State and local
officials; however, DOD will, if directed by the President or SecDef, DOD may be tasked to provide the majority of forces required and have the overall responsibility to defend them.

(2) (d) Space operations. The region of space above the US and cyber-space 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 the HD, through the space control, space force enhancement, and space support mission areas. DOD CIP activities may be closely related to military space operations given that selected military space capabilities systems may be classified as deemed defense critical physical or cyber assets or infrastructure. For HD purposes CIP activities may serve as an approach to protecting and defending our abilities to operate in and through space. In order to deter or preempt attacks and protect our military space assets, DOD conducts space operations as a part of the HLD DCIP function, specifically, space control, space force enhancement, and force application. The CDRUSSTRATCOM is the supported commander for protecting and defending our sovereign right to operate in space and is responsible for identifying, assessing and securing DOD critical assets in space. USSTRATCOM is also responsible for DCIP activities associated with computer network operations (cyber assets) and other DOD information operations—IO, which includes computer network operations. USSTRATCOM may also conduct space operations and IO as a supporting commander to CDRUSNORTHCOM or CDRUSPACOM in the performance of their HLD missions. For more information concerning CAAP see DODD 5160.54; for CIP see DODD 3020. For more information concerning space and information operations see JP 3-14, Joint Doctrine for Space Operations, Joint Doctrine for Space Operations, and JP 3-13, Joint Doctrine for Information Operations.

(2) Antiterrorism/ Force Protection (AT/FP). AT/FP is a high priority item within DOD and measures, considerations and programs should be applied and integrated across the entire HLD mission area. Antiterrorism consists of defensive measures used to reduce the vulnerability of individuals and property to terrorist acts. Force protection consists of offensive and defensive measures and is generally described as a security program developed to protect Service members, civilian employees, family members, facilities and equipment, in all locations and situations. FP is normally accomplished through the planned and integrated application of combating terrorism (antiterrorism and counterterrorism), physical security, operations security, NBC Defense measures and personal protective services and is supported by intelligence, counterintelligence, and other security programs. Although AT activities may be conducted as part of overall FP efforts, for HLS purposes, it will be given special emphasis and may be assessed or reviewed as a separate program. CDRUSNORTHCOM and CDRUSPACOM are responsible for establishing AT/FP policies and programs within their respective AORs for the protection of all assigned and OPCON forces. Programs will also include family members, resources and facilities. Commanders of the combatant commands with functional responsibilities establish AT/FP command policies for the protection of all
assigned forces and coordinate their programs with the appropriate geographic combatant commander or with the Services for the 50 States, US territories and possessions. The Services also institute Service AT/FP programs, and these programs include the reserve components. They are responsible for all AT/FP measures at assigned installations within the 50 states, US territories, or possessions. They will ensure that existing physical security, base defense, and law enforcement programs address terrorism as a potential threat. The services will support geographic and functional combatant commanders in accordance with established policy and directives. For more information on AT/FP see DODD 2000.12 and JP 3-07.2, Joint Tactics, Techniques, and Procedures for Antiterrorism.

(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 lashess 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. FP activities conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable effective employment of forces while degrading the opportunities of the enemy. Activities contributing to the FP mission include, AT, COOP, logistics, medical, legal and safety. DOD’s AT program is one of several security programs that serve as a key element of DOD’s Combating terrorism and FP efforts. The DOD AT program also serves as an integration program for CIP, IO, law enforcement, physical security, CBRNE, and terrorism consequence management and response. DOD AT activities focus on collective, proactive efforts to prevent and detect 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, the CDRUSNORTHCOM and CDRUSPACOM are responsible for establishing and validating AT and FP criteria, setting standards for readiness, and establishing related readiness levels within their respective AORs. Combatant commanders with functional responsibilities establish AT and FP command policies for the protection of all assigned forces and coordinate their programs with the appropriate geographic combatant commander or with the Services for the 50 states, US territories and possessions. The Services are currently responsible for all AT/FP measures at assigned installations within the 50 states, US territories, or possessions to include reserve components. For more information on DOD AT and FP programs refer to DODD 2000.12, August 18 2003 and JP 3-07.2, Joint Tactics, Techniques, and Procedures for Antiterrorism.
Ballistic missile defense (BMD). **BMD is a supporting mission that is embedded within air, land, and maritime defenses.** BMD capabilities are designed to deter, detect, defend against, and defeat enemy ballistic missile threats. Ballistic missile defense of the homeland includes the integration of capabilities to destroy or disrupt enemy missiles in flight or prior to launch. A BMD operational system consists of sensors, weapons, command and control, manning, logistics and C4I systems, which are employed collectively. As with the three primary HD missions, BMD should fully synchronize and integrate offensive and defensive actions and supporting C4I systems to achieve unity of effort. BMD activities may also be closely related to DOD CIP and FP efforts. For example, there may be a requirement to establish a missile defense umbrella over a site that is designated as defense critical infrastructure e.g. a CONUS POE. Space and IO are also considered critical enabling operations for BMD. For example, space based surveillance and sensor capabilities provide ballistic missile early warning, assist in intelligence gathering, and facilitate tracking missiles inbound. IO related computer network defenses ensure critical BMD C4I systems remain protected. Within their respective AORs CDRUSNORTHCOM and CDRUSPACOM are responsible for conducting homeland ballistic missile defenses while CDRUSSTRATCOM is responsible for planning, integration, and coordination of global missile defense operations and support. For more information regarding ballistic missile defense of the homeland see NSPD 23, 16 Dec 02 and the Unified Command Plan (UCP) change 2, 10 January 03.

Information Operations (IO). **IO is a key critical HD enabler and IO activities should be considered always be when integrated when** planning and
executing HL-D missions. Offensive IO activities within the US and its territories or against US persons is not conducted, unless ordered by the President. However IO activities should always be considered when conducting homeland air, land, and maritime defenses. It must be noted that many policy documents discuss cyber defenses associated with HD, but in accordance with joint doctrine on the subject cyber and cyber defenses is interpreted and applied operationally as computer network operations (CNO). CNO consists of computer network attack (CNA) and computer network defense (CND) and is categorized as a core activity of IO. Additionally, IO capabilities—core and related activities—tasks may overlap or become elements of DCIP and AT/FP HLD common functions—other missions supporting HD. For example, the requirement to protect critical DOD assets and infrastructure (both physical and cyber), span IO capabilities associated with computer network defense operations (computer network attack and defense), and cyber defenses. Computer network defense in turn will likely be a critical element of the DCIP efforts to protect DCI. In addition, IO capabilities and activities also serve as critical enablers to our ability to successfully perform AT/FP activities missions associated with HL-D. For example, FP tasks may include installation OPSEC and information assurance (IA) measures and OPSEC and IA are categorized as core and supporting IO capabilities. Other critical IO capabilities that may be leveraged when conducting HL-D offensive and defensive operations include electronic warfare, psychological operations and military deception. Additional physical security is a supporting activity associated with IO supporting capabilities that should be considered when conducting HL-D include physical security, and ISR activities. CDRUSNORTHCOM and CDRUSPACOM conduct IO within their respective AORs for HL-D and will. They should fully coordinate and integrate their efforts with the CDRUSSTRATCOM who has the overall responsibility for defending defense information systems. For more information concerning IO see JP 3-13, Joint Doctrine for Information Operations.

5. Planning Considerations for Homeland Defense Operations

(a) When directed, DOD conducts HL-D activities in accordance with the Unified Command Plan (UCP), and appropriate CONPLANS, and DODDs directives, and SecDef strategic guidance statements. Command relationships will also be specified in appropriate plans and orders.

(1) Operations. As with other joint operations, all HL-D operations are conducted in accordance with extant doctrine and policy. The campaigns may be designed utilizing the 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, transition, provides a flexible planning model to arrange HL-D operations. Figure III-4 portrays examples where HL-D activities could fit in the JP 3-0 notional campaign planning phases.

(2) Simultaneous Operations. HL-D missions and common functions may take place simultaneously with other operations to include CS operations. HL-D operations
are conducted across the range of military operations and unless directed by SecDef, they HD missions will normally take precedence over CS missions. Consequently, there may be competing requirements 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.

(3)c. Public Affairs (PA). HLD activities will draw extensive media attention. Military PA operations activities are subject to approval of the SecDef or the appropriate combatant commander. The Assistant Secretary of Defense for Public Affairs approves and disseminates PA guidance (PAG), PA plans, and PA annexes. Commanders make decisions in an operational environment of complex information demands. A number of news media will already be in an operational area when military forces conduct operations. Free access may be controlled on military installations to ensure OPSEC. The public affairs 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, leaders should always involve their PA personnel when planning HLD 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.

(4)d. Rules of Engagement (ROE). The standing rules of engagement (SROE) for US forces, as delineated in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3121.01 Standing Rules of Engagement for US Forces, establishes fundamental policies and procedures governing the actions to be taken by US commanders during military HLD operations.
Intentionally Blank
CHAPTER IV
CIVIL SUPPORT

1. General

“Everyone knows that the Pentagon is not in the business of providing an armed force for the United States, but when an event occurs we get the phone call and why do we get the phone call? Well, because the Department of Defense is considered the Department of Defense. They know that they’ve got troops. They’ve got people who respond. They’re organized and they can be of assistance.”

Secretary of Defense Donald Rumsfeld
July 2002

a. The Department of Defense—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. Military commanders ensure that DOD resources are used judiciously by adhering to the following principles:

(1) Except in the case of immediate response when local commanders can respond to save lives, prevent human suffering, or mitigate great property damage, 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 a lead federal agency (LFA) and approved by SecDef.

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

(3) The SecDef shall retain control of assigned Title 10 military forces providing civil support CS. (Note: Additionally, 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 Title 32 status (most notably no posse comitatis constraints). Also, most, if not all, deployed NG forces will remain in Title 32 status throughout an event. Therefore, a combined military response made up of Title 10, 14, 32, and/or state active duty forces may be employed in response to individual incidents or events.

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

(5) Unless otherwise directed by the SecDef, or where provided for by law, military operations will have priority over civil support CS missions.

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 or such as disasters and provide support to US civil authorities for domestic emergencies, authorized law enforcement, and other activities that exceed the capability of civilian agencies. This response capability
Chapter IV

described as civil support CS, is one of two homeland security-HS mission areas for DOD.

c. In providing civil support to US civil authorities for domestic emergencies, DOD responds to incidents in accordance with Federal policies, DOD directives, and individual agreements. The Federal Response Plan (FRP) is the primary Federal mechanism through which DOD support is requested. The FRP describes the policies, planning assumptions, and a concept of operations that guide Federal operations following a Presidential declaration of a major disaster or emergency. Additionally, the FRP describes responsibilities, response, and recovery actions of 26 Federal departments and agencies and the American Red Cross (ARC). DOD CS activities normally occur after a presidential declaration of a major disaster or an emergency and are designed to supplement the efforts and resources of State and local governments and non-governmental organizations. CS encompasses missions and functions that foster mutual assistance and support between the DOD and the Federal, state, or local civil government agencies. CS includes planning, preparedness, and the response to civil emergencies and attacks. When performing CS, the US military will respond in support of another lead federal agency (LFA).

c. The most visible, yet infrequent, 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.

The most visible type of assistance DOD provides is support to civil authorities for domestic emergencies or disasters.
d. The majority of CS provided by DOD on a regular basis is to LEAs and may be conducted through individual agreements with the agencies requiring routine support.

2. Civil Support Characteristics

a. **DOD’s planning considerations are key to developing a viable CS strategy.** DOD’s current and future military operations are the primary missions and must take precedence over CS mission areas, unless otherwise directed by SecDef or current law. The combatant commanders responsible for HS, CDRUSNORTHCOM and CDRUSPACOM, incorporate plans for CS by task organizing their commands to accomplish CS missions as well as their military missions. DOD is a signatory to numerous federal response plans as well as various 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 tantamount 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 CM capabilities of DOD, particularly in specialized assets such as the Chemical and Biological Initial Response Force lends a capacity to civilian agencies that may not otherwise have the means to manage a CBRNE event. By exercising with civil authorities, DOD’s CM capabilities are not only enhanced, but they allow 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 and directives.** 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. Office of the Secretary of Defense (OSD) must also validate RFAs using specific criteria that are discussed later in the chapter.

d. In the event an immediate response is needed, local commanders can utilize the “72-hour rule.” This allows the commander to render assistance in the first 72 hours immediately following an incident without the need for prior approval from OSD. Commanders can respond without a disaster declaration to save lives, prevent human suffering, or mitigate gross property damage. Following the first 72 hours, guidance or approval from higher headquarters is highly encouraged.

e. Unless prior agreements or arrangements are in place with MOUs or MOAs, DOD can only support civil authorities in an immediate response situation or via a validated RFA.

23. Civil Support Missions

a. **Employment of military forces within the US, its territories, and possessions, provided under the auspices of civil support CS, typically falls under the broad mission of military assistance to civil authorities (MACA).** MACA operations, for the purposes of this
publication, consist of three mission subsets and are predicated on the authorities governing their implementation (see Figure IV-1). These mission subsets provide structure in this publication for the discussion and understanding of CS and consist of:

1. Military Support to Civil Authorities (MSCA).
3. Military Assistance for Civil Disturbances (MACDIS).

b. Military Support to Civil Authorities. DOD MSCA support, as shown in Figure IV-2, is the most widely utilized subset of military support and primarily consists of support for natural or manmade disasters and chemical, biological, radiological, nuclear and high-yield explosive consequence management (CBRNE CM). Per execution of the Federal Response Plan and the Stafford Act, the President may direct the military to respond to supplement local, State, and Federal relief efforts in order to save lives, protect property and public health and safety, or lessen or avert the threat of a catastrophe in any part of the United States. MSCA includes but is not limited to natural disasters and emergencies (severe weather, wildland firefighting, earthquakes, animal disease eradication), manmade disasters and emergencies (CBRNE consequence management (CBRNE CM)), terrorist incidents, and special events). MSCA support 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 a 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 major disaster or emergency, there will be a concerted US Government effort to support the affected areas. As a signatory to the FRP, DOD may be asked to provide assistance to the 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, wild land firefighting, and animal disease eradication. When natural disasters occur and military assistance is anticipated, 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. Units supporting the event will also be OPCON to the supported combatant commander.

(2) Special Events. DOD is often asked to provide support to a special event, a planned program of athletic competition and 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. SecDef may also designate non-athletic international or national events to receive military support during special events may also be aligned with military support to civilian law enforcement agencies.

Figure IV-2. Examples of Military Support to Civil Authorities

EXAMPLES OF MILITARY SUPPORT TO CIVIL AUTHORITIES

- Natural Disasters
  - Severe Weather
  - Firefighting
  - Earthquakes

- Special Events
  - Olympics
  - Summits
  - World Fair

- Manmade Disasters
  - CBRNE-CM (1)
  - Terrorist Incident
  - Oil Spill

(1) Chemical, biological, radiological, nuclear, high yield explosive - consequence management.
(2) Military support during special events may also be aligned with military support to civilian law enforcement agencies.
support in accordance with DODD 2000.15, Support to Special Events. Other examples of non-
athletic events include the summits, world fairs and the Boy Scout Jamboree. The LFA for
special events can vary. Special events differ from a NSSE. An NSSE is a specific designation
given by the Secretary of Homeland Security and are led by the US SS.

(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. Therefore, specific attention has been focused on task
organizing within DOD to plan for and integrate its support to a LFA to manage the
consequences of a domestic CBRNE event. The 1999 Unified Command Plan (UCP-99)
established a Joint Task Force – Civil Support (JTF-CS) under CDRUSJFCOM to provide
command and control of assigned DOD forces in support of a large–scale CBRNE incident
within continental United States (CONUS). Forces For Unified Command (Fiscal Year 2003)
reassigned JTF-CS to CDRUSNORTHCOM.

c. Military Support to Civilian Law Enforcement Agencies (MSCLEA). MSCLEA includes
types of support to civilian law enforcement agencies (LEAs) as shown in Figure IV-3. The use
of the military in law enforcement roles is generally a sensitive topic and significant restrictions
apply to such use. Military forces performing in this role may work under several LFAs to
include DHS, or FBI/DOJ and may be armed depending on the circumstances. The Secretary of
Defense 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
counterdrug operations, maritime security and general support (training support to law
enforcement agencies / loan of equipment/personnel and expert advice).

(1) Military support to civilian LEAs may include, but is not limited to: National
Special Security Events NSSEs, support to counterdrug operations, support for combating
terrorism, military working dog (MWD) support, CIP and General Support (training support to
law enforcement agencies / national critical infrastructure (NCI)), protection loan of equipment /
personnel and expert advice).

(2) Antiterrorism (AT) Support. Acting through the Federal Bureau of Investigation
(FBI), the Attorney General, in cooperation with other federal departments and agencies,
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 law enforcement agencies (LEAs) during the crisis
management CM portion of a response. If there is a credible threat, DOD may also be requested
to support LEAs in the prepositioning of forces. Under this type of support, specific rules on
for the use of force (RUF) must be established and approved. In the absence of preexisting RUF,
such as are contained in DODD 5210.56, requests for RUF for CS missions will be sent through
the combatant commander to DOD for development and approval. For more information on AT
see JP 3-07., Joint Tactics, Techniques and Procedures for Antiterrorism
National Special Security Events (NSSEs) are events of such national significance that require greater Federal visibility. NSSE is a designation that was established per PDD 62 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 DHS, Homeland Security, in consultation with the HSC, shall be responsible for designating events as NSSEs in conjunction with the Attorney General, makes recommendations to the Office of Homeland Security on which events warrant NSSE designation. The United States Secret Service, a subordinate element of the DHS, is the LFA for NSSE-designated events. Special events, including NSSEs are ranked in magnitude and specific examples include the State of the Union Address, Salt Lake City Olympics, and Democratic and Republican National Conventions.

Historical examples of NSSEs include the Olympic Games.

Counterdrug (CD) 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. The five goals of the national drug control strategy provide a common framework for all US agencies involved in the collective effort to reduce illegal drug use and its consequences. Only a comprehensive planning process at the strategic (national), operational, and tactical (regional) levels can provide the means to reach this goal. The nature of the CD planning should be joint, multinational, and interagency, thus requiring close coordination with all participants. In performance of CD operations DOD will be in support of another LFA. The Drug Enforcement Agency (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) National Critical Infrastructure Protection (CIP) (NCI). While DOD is responsible for DCIP, there may be instances where the President and SecDef will instruct DOD to provide support to other LFAs in their roles to protect NCI. This support can be in many forms but is normally associated with support missions associated with disasters, emergency relief, crisis management CrM and consequence management CM activities. NCI_Critical infrastructure is comprised of those physical and cyber-based 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-4. Many of the NCI nation’s critical infrastructure have historically been physically and logically 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, and physical and cyber as well as actual attack. Addressing these vulnerabilities will require new and flexible approaches spanning both the public and private sectors, to protect both domestic and international security. Our economy is also increasingly reliant upon interdependent and cyber supported infrastructures. Non-traditional attacks on these infrastructures and other information systems may be capable of significantly harming both our ability to project military power and the national economy. Adversaries, whether nations, groups or individuals, will likely attempt to employ asymmetric approaches to impair or destroy NCI critical infrastructure by avoiding our strengths and exploiting our actual or perceived weaknesses.

(4) Maritime Security. The USCG, when operating under the 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; explosive ordnance disposal teams for port security; or mine clearance operations. Certain law enforcement activities, such as boardings, will require the embarkation of law enforcement detachments aboard US Navy ships.

(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 the DODD 5525.5 for MSCLEA, 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.

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

34. Associated Terms: Supporting Operations and Enabling Activities

When performing missions associated with CS, DOD will always serve in a supporting role. The following, although not inclusive, describes supporting operations and enabling activities commonly associated with CS MACA missions. Numerous interagency plans and policy documents define DOD's relationship with the LFA. Homeland Security Presidential Directive HSPD-5 states that the United States Government shall establish a single, comprehensive approach to domestic incident management that treats crisis (CrM) and consequence management (CM) as a single integrated function. The following describes the terms activities associated with the management of CS incidents.

a. Incident Management. A single national comprehensive approach to preventing, preparing for, responding to, and recovering from terrorist attack, major disasters, and other emergencies. 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 at this level incident management will eventually include both crisis and consequence management activities employing a cyclical approach. Currently DOD policy addresses crisis and consequence management as separate activities.

MILITARY ASSISTANCE FOR CIVIL DISTURBANCE OPERATIONS

Figure IV-3. Military Assistance for Civil Disturbance Operations
Chapter IV

b. (1) Crisis Management. 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. Presidential Decision Directive PDD-39, US Policy on Counterterrorism, designates the DOJ, specifically the FBI, as the LFA for crisis management CrM. The Federal government exercises primary authority to prevent, preempt, and terminate threats or acts of terrorism and to apprehend and prosecute the perpetrators; state and local governments provide assistance as required. Crisis management 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 crisis management and consequence management.

Figure IV-4. Relationship Between Crisis Management and Consequence Management.
c. Consequence Management. CM includes those actions required to manage and mitigate problems resulting from disasters and catastrophes, including natural, manmade, or terrorist incidents. Such services may include the range of ESFs described in the FRP. It also may include continuity of operations—COOP / continuity of government—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 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. FEMA has the primary responsibility for coordination of federal CM assistance to state and local governments. See Figure IV-6.

d. Technical Operations. Based on the situation, a federal crisis management—CrM response may be supported by technical operations and by federal consequence management—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. The LFA for technical operations depends upon the material involved and the location of the incident. Other federal agencies supporting technical operations include Defense, Energy, Health and Human Services, and the Environmental Protection Agency (DOD, DOE, DHHS, and the EPA).

c. Critical Infrastructure Protection (CIP). 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 is comprised of 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 require new and flexible approaches spanning both the public and private sectors to protect both domestic and international security. Our economy is also increasingly reliant upon interdependent and cyber-supported infrastructures. Non-traditional attacks on these infrastructures and other information systems may be capable of significantly harming both our ability to project military power and the national economy. Adversaries, whether nations, groups or individuals, will likely attempt to employ asymmetric approaches to impair or destroy critical infrastructure by avoiding our strengths and exploiting our actual or perceived weaknesses.
4.5. Department of Defense Civil Support Process

a. Functionality. In January 2003, pursuant to the National Defense Authorization Act of Fiscal Year 2003, the Secretary of Defense—SecDef—established, the Office of the Assistant Secretary of Defense for Homeland Defense (ASD(HD)). In addition to overseeing homeland defense activities, the Secretary of Defense—SecDef—has vested the roles and responsibilities associated with the DOD Executive Agent for MSCA and MACDIS with the ASD(HD). The Secretary of Defense also transferred the functions and associated resources of the Army’s Office of Director of Military Support (DOMS) to the Joint Chiefs of Staff. This staff section resides in the J-3 Current Operations Directorate and is known as the Joint Director of Military Support (JDOMS). The ASD(HD) exercises policy for DOD CS missions. JDOMS producres military orders and the appropriate military commander will exercise C2 of military forces. Figure IV-8 depicts how CS responsibilities were transferred from the Army and DOMS to the ASD(HD) and JDOMS. It also outlines specific functions and tasks the ASD (HD) and JDOMS will perform in the event DOD receives a request for assistance.

EXAMPLES OF CRITICAL INFRASTRUCTURE

Vital Human Services
Telecommunications
Electric Power Systems
Transportation
Gas and Oil Transportation
Water Supply System
Emergency Services
Continuity of Government Infrastructure

Selected criteria infrastructure may be designed as essential to HD missions

Figure IV-5. Examples of Critical Infrastructure.

eb. Command, and Control and Coordination
(1) DOD forces providing CS will always remain under military command and control. The SecDef or his designee will validate any requests for assistance. The ASD(HD) is the executive agent for MSCA and MACDIS. In March 2003, the roles and responsibilities associated with the DOD Executive Agent for MSCA and MACDIS were transferred from Secretary of the Army to the ASD(HD). SecDef also transferred the functions and associated resources of the Army’s Office of the Director of Military Support (DOMS) to the Joint Chiefs of Staff office of the Joint Director of Military Support (JDOMS). Guidance from the SecDef or the ASD(HD) is translated into operational orders developed by the 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-76 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 SecDef authorizes specific approval authority for the deployment of forces for certain of MSCLEA and MACA operations. Specific command and control arrangements for CS operations are addressed in Chapter II, Command Relationships and Interagency Responsibilities.

**Figure IV-6. Request for Assistance**
Chapter IV

(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 ExecSec, DOD will provide assistance. 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 its C2 headquarters, JTF-CS, which will exercise OPCON over designated DOD forces. The defense coordinating officer (DCO) remains the on-site DOD single point of contact for requests for DOD assistance in accordance with the INRP / FRP.

(3) While executing CS missions, DOD personnel work closely with civilian government officials from federal, state, and local governments, as well as volunteer and non-governmental 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.

bc. Requests for assistance. As previously outlined, DOD is always in a supporting role when performing CS operations. In accordance with the INRP / FRP, DOD will provide equipment or assets when the mission does not interfere with its military functions. The type and extent of requests for DOD assistance is wide-ranging and in order to expedite DOD support, requests for assistance (RFAs) must be submitted through the Executive Secretary (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. Once DOD accepts an RFA, JDOMS will draft the military order and forward it to the Office of the Secretary of Defense for approval. Given that most civil support CS missions involve life-saving responses, this order process is rapidly executed to expedite the movement of forces and prompt support. Except in cases of immediate response, DOD cannot provide MACA without an official request from another federal agency or direction from the President. The most visible, yet infrequent, type of assistance DOD provides is support to civil authorities for domestic emergencies or disasters. However, the majority of CS provided by DOD on a regular basis is typically some form of MSCLEA. The type and extent of RFAs is wide-ranging.

c. Command and Control

(1) DOD forces providing CS will always remain under military command and control. The SecDef or his designee will validate any requests for assistance. The ASD(HD) is the executive agent for MSCA and MACDIS. Guidance from the SecDef or the ASD(HD) is translated into operational orders developed by the JDOMS. USNORTHCOM and USPACOM are the supported combatant commanders within their AORs for mission execution. The SecDef only authorizes specific approval authority for deployment of forces for certain of MSCLEA and MACA. Specific command and control arrangements for CS operations are addressed in Chapter 2.

(2) DOD support to a CBRNE consequence management situation is similar to DOD support for routine MSCA operations. Upon a validated request from the lead federal agency to the ExecSec, DOD will provide specialized assistance in response to a CBRNE situation. USNORTHCOM and USPACOM, will serve as the supported commanders within their AORs.
for CBRNE CM activities. As reflected in Figure IV-9, for large CBRNE CM events within CONUS, USNORTHCOM may deploy their command and control headquarters, JTF - Civil Support, who will exercise OPCON over designated DOD forces. The DCO remains the DOD single point of contact for requests for assistance in accordance with the FRP.

ad. Mechanisms. DOD is always in a supporting role when providing CS, thus all military assistance must be requested in some fashion, except for instances of immediate response.

(1) MOA/MOU. While the majority of CS is coordinated through the EXECSEC, there are some instances in which DOD provides support based upon existing interagency MOAs/MOUs. Numerous interagency MOA/MOU provide the basis for coordinated responses when situations warrant.

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

(a) Federal Response Plan. The most prominent of CS plans is the FRP, which is still the primary federal mechanism through which DOD support is requested for domestic emergencies. The FRP 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 FRP is coordinated and managed by FEMA and is the result of agreements between FEMA and the primary and supporting federal agencies responsible for providing disaster relief support. The primary agency for resource support under the FRP is the General Services Agency. 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 FRP: FEMA, National Aeronautics and Space Administration, National Communications System and the Office of Personnel Management. DOD resource support under the FRP 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) Initial National Response Plan. HSPD-5 directed the Secretary of Homeland Security to develop and administer a 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 FRP and the other family of emergency response plans (U.S. 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) will eventually be integrated into the NRP. However, at present, only an INRP has been produced. While this document will serve as a bridge between the current family of documents and the NRP, the current family of response plans, including the FRP, remains in effect until a final
NRP has been developed and approved. At that time, the NRP will supersede existing interagency plans, unless otherwise specified. In addition to consolidating federal plans, other modifications within the INRP 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 INRP will be addressed in Joint Pub 3-26.2, Joint Doctrine for Civil Support.

65. Process d. Planning Considerations for Civil Support Operations

a. When directed, DOD responds to domestic emergencies in accordance with applicable DODDs, contingency, and Federal response plans. The most prominent of these plans is the Federal Response Plan, which is coordinated by DHS/FEMA. The FRP provides the mechanism for coordinating delivery of Federal assistance and resources to augment efforts of State and local governments overwhelmed by a major disaster or emergency, and supports the Stafford Act as amended. Other Federal plans include the Federal Radiological Emergency Response Plan (FRERP), the United States Government CONPLAN, and the Mass Immigration Emergency Plan (MIEP). These plans are activated based on the type and level of emergency. In addition, the Chairman of the Joint Chiefs of Staff has issued CONPLAN 0500, which provides operational guidance on the execution of military assistance to domestic CBRNE-CM situations.

a. Response Channels. While most CS is coordinated through ASD (HD) and the Joint Staff, the military may also respond through other channels. Federal agencies may request DOD support based on interagency memorandum of agreement. For example, under an interagency MOA, the US Navy may deploy oil containment and recovery equipment to support USCG efforts to clean up oil spills. Numerous interagency MOAs provide the basis for coordinated responses when situations warrant. In addition, United States Army Corps of Engineers (USACE) has civil authority, responsibilities, capabilities, and unique funding within the DOD for CS missions.

b. Operation Stages. CS operations are normally conducted in three stages: response, recovery, and restoration. Response operations focus on those life-saving and sustaining functions required by the population in the disaster area. DOD normally provides support in five phases of CM support: situation assessment and preparation, deployment, assistance to civilian authorities, transition to civilian agencies, and redeployment. 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. Restoration is a long-term process that returns the community to pre-disaster normalcy. Military forces normally redeploy as operations transition from the response to the recovery stage; normally the military role in civil support CS operations is transferred to civilian organizations as soon as practicable. This is in keeping with the policy of DOD being the responder of last resort and "last in, first out."
units and support such as transportation, equipment, and supplies that must be balanced with commitments elsewhere in the world. Asset-sourcing conflicts must therefore be quickly resolved to prevent delays in responding to time-sensitive requirements.

**ce. 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. Depending on the type of operation, legal ramifications are present; therefore, comprehensive legal reviews of CS plans are required.

1. Sound legal advice during MACA operations will ensure that the application of military capabilities and resources are 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 provides specific legal guidance for DOD CS. JA’s 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 counterdrug 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.

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

1. **MACA:** The standing rules of engagement as delineated in CJCSI 3121.01A *Standing Rules of Engagement for US Forces(U)*, do not apply to US forces conducting MACA 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 (e.g. FBI, US Customs Service). Forces conducting counterdrug 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 judge 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 used 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 via 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.

df. Concurrent Assistance to Civilian Agencies. Military responses to a credible threat or acts of terrorism may require both crisis management CrM and consequence management CM operations. These operations may often overlap. The DOJ/FBI is the overall LFA in preventing or resolving threats involving terrorism and for crisis response throughout a terrorist situation threat or act. FEMA leads consequence management CM operations and is the LFA for emergency response efforts to lessen or mitigate the consequences of attacks or incidents. In multiple situations, CM may include pre-event planning for one incident while conducting post-event operations of another. DOD direct support for CM is provided to FEMA or an INRP / FRP primary agency. While DOD forces support consequence management activities they may also support crisis management efforts. Under these circumstances supporting elements should coordinate, integrate and synchronize their activities and operations. For more detailed guidance on CS operations see JP 3-36.2, Joint Doctrine for Civil Support.

eg. Public Affairs (PA). CS usually draws extensive media attention. Military PA operations activities are subject to approval of the lead agency LFA. Military public affairs officers (PAOs) operate in an interagency environment, with emphasis on cooperation, coordination, and unity of effort. Commanders operate in an environment of complex information demands. Free access for the media is normally regulated to ensure operational security, however the public’s impression of the assistance effort depends to a great extent on the
media. This perception also influences the cooperation and coordination between commanders and civilian leaders. Positive public support is a force multiplier that facilitates mission accomplishment. Lack of public support, on the other hand, can seriously impede the effectiveness and efficient employment of military forces during the execution of CS missions. The PAO is a key member of the commander’s staff and advises the commander on the information demands anticipated, information strategies available, and the effect of the communications effort. PA personnel should be involved in as many of the planning phases as is consistent with security requirements. News media access to CS operational areas is subject to the approval of the lead civilian agency. PAOs operate under the conditions imposed by the government agency that has jurisdiction. The lead Federal agency LFA has release authority. The military must coordinate all PA activities with the lead Federal agency LFA and comply with its PA guidance. For further details, 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 (FCO), 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.

f. Coordination. In CS, DOD personnel work closely with civilian government officials from Federal, State, and local governments, as well as volunteer and non-governmental 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. Refer to JP 3-08, Interagency Coordination During Joint Operations, for further guidance.

g. Rules on the Use of Force (RUF) Guidelines and Rules of Engagement (ROE). Depending on the type of civil support mission, different RUF or ROE apply:

(1) MACA: The standing rules of engagement (SROE) as delineated in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3121.01 Standing Rules of Engagement for US Forces, do not apply to US forces conducting MACA 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 on the Use of Forces”. There is a presumption that units deployed to sites of a CBRNE situation will not carry arms. As authorized by the SecDef, units may deploy to sites of CBRNE situations with their weapons stored in an appropriate unit storage container to cover possible follow-on assignments where weapons are authorized. Military chains of command are responsible to ensure that weapons and ammunition are properly stored and physically secured at the site of the CBRNE incident.
(2) MSCLEA: Forces deployed to assist LEAs may or may not be armed depending on the situation. These forces will adhere to the ROE/RUF as designated in the deployment order or MOA with the supported Federal law enforcement agency (e.g. Federal Bureau of Investigation, Immigration and Naturalization Service, US Customs Service). Forces conducting counterdrug 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 of GARDEN PLOT).

(4) In CS, appropriate military capabilities are applied prudently and with restraint. RUF and ROE are more 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) Military forces involved in CS should be trained in RUF and ROE before operations begin. Military leaders ensure that forces clearly understand RUF and ROE. Commanders should consult their Staff Judge Advocates regarding the implementation of any training program on RUF and ROE. These should be continually stressed during the operation. Written guidance, frequent information update briefings, and brief-backs are methods used to ensure that military forces understand procedures.

6. Environmental Considerations. Commanders should make environmental considerations an integral part of the mission planning and operational decision-making process. All joint operations within the United States, US and US territories should 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.”

6. Authorities

a—i. Legal considerations. The authorities governing the employment of U.S. military forces in civil support operations consist of Federal laws, executive directives, DOD plans and policies, and other directives, instructions and regulations. Depending on the type of operation, unique legal ramifications are present; therefore, comprehensive legal reviews of CS plans are required. Sound legal advice during MACA operations will ensure that the application of military capabilities and resources are within the constraints of the law. Commanders involved in CS should staff plans, policies, programs, exercises, funding, operations, constraints, and limitations with their staff judge advocates (SJAs) to ensure conformity with legal requirements. Federal, State, and local governments execute US laws with the assistance of LEAs. The Domestic Operational Law (DOPLAW) Handbook for Judge Advocates provides specific legal guidance for DOD civil support.
b. Limited military support to LEAs is allowed under other laws such as Title 10 United States Code (USC) Sections 371-381. Under these laws, the military may share certain information and provide equipment, facilities, and other services to LEAs. The 1991 National Defense Authorization Act allows certain types of military support for the national counterdrug effort. The authority and funding for these activities have been extended in subsequent authorization acts so that they are still current, and they 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, Legal and Policy Documents.
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 homeland security mission areas. These range from the US Constitution to the Contingency Planning Guidance (CPG). Figure I-6 depicts a number of the key documents.

a. The Constitution. The Preamble states the purposes of the Constitution is 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 homeland security activities 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 homeland security missions:

1. President George W. Bush’s Homeland Security Presidential Directive (HSPD)-1, Organization and Operation of the Homeland Security Council (October 29, 2001) established the Homeland Security Council (HSC) to ensure coordination of all homeland security-related activities among the executive departments and agencies and promote the effective development and implementation of all homeland security 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 colors.

4. Homeland Security Presidential Directive / HSPD-4. National Strategy to Combat Weapons of Mass Destruction (December 2002). HSPD-4 established 3 pillars for our national strategy to combat WMD. They are: 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.

Appendix A

directive describes the way federal departments and agencies will prepare for such responses, including prevention activities during the early stages of a terrorist incident.

(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.

(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. In that terrorist seek to destroy, incapacitate, or exploit critical infrastructure and key resources to threaten national security, mass casualties, weaken our economy, and damage public morale and confidence, such capabilities must be protected. Critical infrastructure and key resources provide the essential services that underpin American society. This directive identifies roles and responsibilities of the Secretary of Homeland Security and recognizes the 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.


(210) Presidential Decision Directive 62, Combating Terrorism (pre-September 11, 2001) created a more 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.

(3) Presidential Decision Directive 63, Critical Infrastructure Protection. was also a pre-September 11, 2001 effort to provide guidelines for the critical infrastructure protection. This directive established the organization and structure for specific sectors and functions, naming lead agencies for sector liaison.
(411) 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.

(512) 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 mission areas for the HS mission. 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 missions are compatible with the DOD operational framework for homeland security that is discussed in this publication. To better facilitate the overarching homeland security mission, Congress established the Department of Homeland Security by merging 25 agencies into a single department.

(613) Homeland Security Act of 2002 established a new Department of Homeland Security (DHS) to coordinate all federal HS efforts to protect the nation against threats to the homeland. It changed the policy and interagency organizational environment for affected departments and agencies, including the FEMA. To better facilitate the overarching HS mission, Congress established the DHS by merging numerous agencies into a single department.

(14) 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 unearther during a criminal investigation.

(715) 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.

(16) 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, a LFA may request the support of DOD without a Presidential declaration of an emergency as required by the Stafford Act.

(817) National Strategy for Combating Terrorism. Expands on the National
Strategy for Homeland Security 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.

(918) 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 National Strategy for Homeland Security NSHS. It identifies a clear set of national goals and objectives to achieve our protection goals. The strategy identifies 13 critical infrastructure sectors. Key asset protection represent 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.

(4019) National Strategy for Securing Cyberspace, is an implementing component of the National Strategy for Homeland Security NSHS. The National Strategy complements it for the Physical Protection of Critical Infrastructure and Key Assets. 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 government, 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.

(4420) Posse Comitatus Act (PCA) (Title18 USC 1385). This federal statute that places limits on the use of military for civilian law enforcement. It specifically prohibits the willful use of any part of the US Army or the US Air Force to execute the laws unless an emergency situation exists (note: The PCA does not apply to the US Coast Guard USCG or National Guard NG forces acting in State Active Duty or Title 32 status). Since its passage in 1878, the PCA has been interpreted to impose significant restrictions on the use of federal military forces to perform civilian law enforcement functions except as authorized by Congress or the Constitution. Specifically prohibited direct assistance includes: (1) interdiction of a vehicle, vessel, aircraft, or other similar activity; (2) search or seizure; (3) arrest, apprehension, stop and frisk, or similar activity; or (4) use of military personnel for surveillance or pursuit of individuals, or as undercover agents, informants, investigators, or interrogators. Conversely, there are several forms of direct assistance by military personnel that are permitted under the PCA, all of which are described in DODD 5525.5, DOD Cooperation with Civilian Law Enforcement Officials. The terms of the PCA apply to the US Army and the US Air Force. DOD policy extends this prohibition to the US Navy and Marine Corps. The PCA
prescribes criminal penalties for its violation. Exceptions to the Posse Comitatus Act include:

(a) National Guard NG forces operating under state active duty or Title 32,
(b) Federal troops acting pursuant to the presidential power to quell domestic violence insurrection,
(c) Aerial photographic and visual search and surveillance by military personnel,
(d) Congressionally created “drug exception”,
(e) The USCG when operating in its maritime law enforcement role.

Title 10 U.S. Code 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. Specifically, Title 10 USC 375 directs the 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.”

Title 14 USC 2, 19, 89, 141, and 143 stipulates the statutory authorities of the USCG during HS missions.

Title 32 U.S. Code, National Guard. Title 32 provides guidance on the National Guard. The guidance addresses organization, personnel, training and Service, Supply, and Procurement. Specifically, this statute permits the state governor to activate the National Guard forces in his state and exercise command over them, and under certain circumstances associated with HLS missions, allows control to remain under the governor while the Federal Government provides funding. Specifically, statutes in Title 32 US Code 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 (CD) missions, and the President of the Untied States directed airport security mission.

Authorization and Appropriation Legislation by Congress. Specific acts, such as the National Defense Authorization Act (NDAA) for 2003, may require or permit the DOD to conduct HLS activities. The 1991 NDAA, for example, permitted certain counter-drug activities for a given period of time.
Appendix A

(24) The National Security Strategy and The National Military Strategy. The NSS provides overarching guidance to the DOD while the NMS interprets that and other guidance to the Nation’s Armed Forces. The NSS and the NMS continue to reflect the first and fundamental commitment to defend the Nation against its enemies.

2. Department of Defense Policy and Guidance

a. Implications. Specific authority for HLS missions are contained in federal and state law and policy documents. These form the basis for the development of Department of Defense-DOD guidelines. These guidelines are promulgated in a variety of methods that include national strategy documents, planning guidance, and Department of Defense directives (DODDs). These policy documents are consistent with and complimentary to the Federal statutes and guidelines discussed earlier in this chapter. DODDs specifically address missions for homeland defense HD and civil support CS operations.

b. Key DOD Guidance. The following discussion identifies a number of key documents that will make the commanders and planners more aware of existing material that may assist in the planning and execution of homeland security HS missions. The grouping is not all-inclusive but contains key documents to aid the operator.

(1) The National Security Strategy (NSS) and The National Military Strategy (NMS). The NSS provides overarching guidance to the Department of Defense while the NMS interprets that and other guidance to the Nation’s Armed Forces. The NSS and the NMS continue to reflect the first and fundamental commitment to defend the Nation against its enemies.

(21) Unified Command Plan (UCP). The UCP provides guidance to all combatant commanders, establishes their missions and responsibilities and delineates the general geographic area of responsibility AOR for combatant commanders.

(32) Defense Planning Guidance (DPG). The DPG establishes four defense strategy goals: assure, dissuade, deter, followed by defeat. The goals are articulated in a planning construct of deterring forward and winning decisively while defending at home. Additionally, the DPG establishes the Department of Defense’s most important mission as the defense of the US homeland. It additionally points out that the Department must establish an optimal organizational architecture to manage homeland defense, civil support and emergency preparedness missions to ensure DOD’s interoperability with and support to other Federal, State and local agencies. Strategic Planning Guidance (SPG). The SPG provides direction for DOD components to develop the Future Years Defense Program and the Presidents budget submission. The four defense policy goals are: 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 list the priorities of SecDef: winning the Global War on Terrorism, strengthening combined/joint war fighting capabilities, transforming the joint force, optimizing intelligence capabilities, counter proliferation, 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.

(4) Contingency Planning Guidance. The CPG reflects the Secretary of Defense's SecDef written policy guidance to the Chairman of the Joint Chiefs of Staff (CJCS) for contingency planning. It is issued with the approval of the President after consultation with the CJCS and provides the focus for the guidance in the NSS and DSPG and is the principal source document for the Joint Strategic Capabilities Plan.

(5) DODD 2000.12, DOD Antiterrorism Force Protection (AT/FP) Program. This directive updates policies and assigns responsibilities for implementing the procedures for the DOD AT/FP Program. It establishes the CJCS as the principal advisor and focal point responsible to the SecDef for DOD AT/FP issues. It also defines the AT/FP responsibilities of the military departments, commanders of combatant commands, and defense agencies. It guidelines are applicable for the physical security of all DOD activities both overseas and in the homeland 50 United States, its territories, and possessions.

(5) DODD 3020.XX, Defense Critical Infrastructure (Draft). This directive establishes policy and assigns responsibilities for DCI activities as they apply to the DOD, and authorizes the 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. JP 3-26 will reflect the language in this DODD regardless of the status of the DODD when this publication is promulgated.

(6) DODD 3025.1 Military Support to Civil Authorities and DODD 3025.12, Military Assistance for Civil Disturbance. DODD 3025.1 and DODD 3025.12 provide guidance on civil support CS activities. The LFA may request DOD assistance for the civil support CS missions, both natural and man-made disasters. All requests for DOD assistance enter through the Executive Secretary EXECSEC. (a) Immediate Response. When imminently serious conditions resulting from any civil emergency or attack may require immediate action, local military commanders and responsible officials o-f-of the DOD components may take such actions as may be necessary to save lives, prevent human suffering, and mitigate great property damage.

(7) DODD 3025.15 Military Assistance to Civil Authorities (MACA). This directive governs all DOD military assistance to civil authorities 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. The SecDef must approve all requests for assistance. The CJCS assists the SecDef in implementing the DOD operational response to acts or threats of terrorism.

(8) 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.

(9) DODD 5160.54, Critical Asset Assurance Program (CAAP). This directive expands the requirement to identify critical assets and assure 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.

(10) 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.

(11) Chairman of the Joint Chiefs of Staff (CJCS) Concept Plan (CONPLAN) 0500, Military Assistance to Domestic Consequence Management Operations in Response to a Chemical, Biological, Radiological, Nuclear, or High-Yield Explosive Situations. This plan provides the SecDef with a wide range of military options to assist in the domestic CM operations of a CBRNE situation. 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.

(12) CJCSI 3110.16, Military Capabilities, Assets, and Units for Chemical, Biological, Radiological, Nuclear, and High Yield Explosive 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 involving CBRNE. Although an actual CBRNE incident would involve a large array of DOD assets, this instruction primarily focuses on CM technical support and unique CM capabilities that are not generally found throughout the force. This instruction lists selected CBRNE-CM capabilities, assets and units by Service.

(13) CJCSI 3121.02, Rules on 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 counterdrug operations in the US.

(14) CJCSI 3125.01, Military Assistance to Domestic Consequence Management Operations in Response to Chemical, Biological, Radiological, Nuclear, or High-Yield Explosive 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.

(15) CJCSI 3209.01, Critical Infrastructure Protection (Draft).
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.

(16) CJCSI 3710.01A. DOD Counterdrug Support. This instruction promulgates SecDef delegation of authority to approve certain counterdrug 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.
APPENDIX C
COMBAT SUPPORT AGENCIES AND CAPABILITIES

Combat Support Agencies (CSAs) provide direct support to the Combatant Commands performing HLS during wartime or emergency situations and are subject to evaluation by the Chairman of the Joint Chiefs of Staff (CJCS). Figure C.B-1 illustrates where each of the 7 combat support agencies are nested within DOD and how they are related to other defense agencies.

The following addresses general and specific missions, functions and capabilities of DOD combat support agencies (CSAs) in support of HLS activities.

1. Defense Information Systems Agency (DISA)

DISA is responsible for planning, developing and supporting command, control, communications, and information (C4I) systems that serve the needs of the National Command Authority, President and SecDef under all conditions of peace and war. It supports the Office of the Secretary of Defense (OSD), the Chairman of the Joint Chiefs of Staff (CJCS), the Combatant Commanders, and the Defense Agencies. For HLS operations, DISA performs a number of core C4I-supporting missions which include...
communications, joint command and control, defensive information operations, combat support computing and joint interoperability support. For more information on DISA core missions see their home page at www.disa.mil.

2. Defense Intelligence Agency (DIA)

a. DIA is responsible for satisfying military and military-related intelligence requirements for the Secretary of Defense SecDef, the Chairman of the Joint Chiefs of Staff 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. They provide military intelligence to warfighters, defense policymakers and force planners, in the Department of Defense DOD and the Intelligence Community.

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

c. DIA is headquartered at the Pentagon in Washington, D.C., with major operational activities at the Defense Intelligence Analysis Center (DIAC), Washington, D.C., the Armed Forces Medical Intelligence Center (AFMIC), Frederick, Maryland, and the Missile and Space Intelligence Center (MSIC), Huntsville, Alabama.

d. The DIA possesses subject matter experts skilled in the areas such military history and doctrine, economics, physics, chemistry, world history, political science, bio-sciences, and computer sciences to name a few. 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 Production (DI), particularly the Defense Warning Office (DWO) assesses both the most likely developing threats and the high impact threats to military capabilities, transformation goals, and US national infrastructures upon which the military depends for stateside operations, training and deployment.

e. DIA responds to the needs of the customer from the President of the United States to the soldier in the field. They cover all aspects of military intelligence requirements—from highly complex missile trajectory data to biographical information on foreign military leaders. DIA’s Disruptive Technology Innovations Partnership (DTIP) program provides HS, HD, and US infrastructure sectors with actionable intelligence assessments for mitigating 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 in these target sets, to include: C4ISR, US stateside military installations, electric power, water supply, petroleum, gas, transportation, finance, telecommunications, government, industrial, agriculture, health, and human environment infrastructures.
e. DIA/J2 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 that includes terrorism, FP and WMD.

3. Defense Logistics Agency (DLA)

DLA provides worldwide logistics support for the missions of the Military Departments and the Unified Combatant Commands under conditions of peace and war. Specifically: It also provides logistics support to other DoD Components and certain Federal agencies, foreign governments, international organizations, and others as authorized. 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), organizations, and others as authorized. DLA's origins date back to World War II when America’s huge military buildup required the rapid procurement of vast amounts of munitions and supplies. 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.

a. DLA provides logistics 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 federal agencies have the lead and DOD has a supporting role until tasked. However, DLA must be prepared to provide support if tasked by the DOD Executive Agent, ASD(HD), JDOMS or USNORTHCOM. When directed by the authorities mentioned above, DLA provides DOD backup support.

d. DLA provides support to USNORTHCOM in the form of a liaison officer (LNO) who works directly with USNORTHCOM J-4, Logistics and Engineering Directorate and through a DLA Contingency Support Team (DSCT) when activated. The DLA LNO to USNORTHCOM is the primary focal point for disseminating, coordinating, and tracking CDRUSNORTHCOM issues and concerns to and from DLA. DLA will provide forward deployed DCST (as required) in the USNORTHCOM AOR to meet real world and contingency requirements (as stated in the current MOA) 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 http://www.supply.dla.mil/CustomerHandbook/index.asp. A toll-free customer number is also available at 1-877-DLA-CALL.
4. National Security Agency (NSA)

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

a. The information assurance mission provides the solutions, products and services, and conducts defensive information operations(IO), to achieve information assurance for information infrastructures critical to U.S. national security interests.

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

c. NSA/CSS Central Security Service executes signals intelligence (SIGINT) and information systems security activities and conducts related activities, as assigned by the Secretary of Defense, 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 the National Security Agency NSA.

5. Defense Contract Management Agency (DCMA)

DCMA works directly with defense suppliers to help ensure that DOD, Federal, and allied government supplies and services are delivered on time, at projected cost, and meet all performance requirements. DCMA performs all contract audits for DOD and provides accounting and financial advisory services regarding contracts and subcontracts to all DoD components responsible for procurement and contract administration. Within the Defense Critical Infrastructure Program, 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.dcma.mil.

6. National Imagery and Mapping Agency (NIMA) National Geospatial Intelligence Agency (NGIA)

NIMA-NGIA is the agency a National Intelligence and Combat Support Agency that 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. The following outlines other NIMA-NGIA activities and support.

(1) Supports customers in the defense, law enforcement, intelligence, Federal and civil communities for Homeland Security (HIS) missions with its analytic GEOINT capabilities.

(2) Supports defense missions for the Common Operating Picture (COP),
military operations assuredness, and **force protection (FP)** by building integrated datasets to support the **Homeland Security (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 **crisis response (CrM) and consequence management (CM)**.

(3) In concert with other **Federal (Fed)** partners, serves as the imagery and geospatial data broker, integrator, and consolidator in building a single **Homeland Security (HS) database** to support domestic situational awareness, **crisis (CrM) and consequence management (CM)**, and critical infrastructure protection (**CIP**).

(4) Provides integrated geospatial information in support of the planning and execution of **Homeland Security (HS) exercises** where there is **Fed**, DoD, state and local government participation.

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

(6) Provides direct, tailored geospatial information support to the border and transportation communities.

(7) Provides **Geospatial Intelligence Support Teams (NST) national intelligence support teams (NIST)** to **Northern Command (USNORTHCOM) and the Department of Homeland Security (DHS)**. These NISTs provide day-to-day GEOINT support to the **command** with the capability to reach back to **NIMA–NGIA** for requirements that exceed the capacity or capability of the team at the **command**.

7. **Defense Threat Reduction Agency (DTRA)**

   a. As a **combat support agency (CSA)**, DTRA provides services and support to DOD components. It is ready and responsive to operating forces in war and threats to national security. DTRA offers a range of capabilities relating to **chemical, biological, radiological, nuclear, and high explosive weapons of mass destruction (CBRNE WMD)**.

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

      (1) Secure communications

      (2) Rapid reach-back capability

      (3) **Video and Teleconferencing (unclassified 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. The Defense Threat Reduction Agency (DTRA) has the Hazard Prediction and Assessment Capability (HPAC) and Consequence Assessment Tool Set (CATS) to forecast damage such as blast, heat, radiation, and hazardous material release and the effects of unpredictable phenomena such as natural or man-made disasters.

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

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

(3) **Joint Staff Integrated Vulnerability Assessment Teams.** Assess security weaknesses of installations.

(4) **Balanced Survivability Assessment Teams.** Assess security weaknesses of critical facilities.

(5) **Direct Support Teams (DSTs).** Direct operational support to combatant commanders in combating weapons of mass destruction. DSTs can be augmented with any specialty deemed appropriate to meet mission requirements.

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

d. In addition, DTRA operates the Defense Nuclear Weapons School, (DNWS), which offers a range of courses on weapons of mass destruction 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.
Intentionally Blank
The development of JP 3-26 is based on the following primary references:

1. General
   b. EO 12333, United States Intelligence Activities, 4 December 1981.
   d. EO 13010, Critical Infrastructure Protection, 15 July 1996.
   h. Federal Radiological Emergency Response Plan (FRERP) 1 May 1996.
Appendix C


s. National Security Strategy


z. The NORAD Agreement and Terms of Reference, and the CANUS Basic Security Document 100/35.


u. PDD-62, Combating Terrorism, 22 May 1998. (Unclassified Fact Sheet).


w. Title 18 United States Code (USC), Section 1385, The Posse Comitatus Act, 1878.

x. Title 31 USC, Section 1535, The Economy Act.
References

- **yygg.** Title 42 USC, Section 5121, *The Stafford Act, as amended, 320 October 2000.*
- **zhh.** Title 10, USC, *Armed Forces.*
- **aaii.** Title 14, USC, *United States Coast Guard.*
- **bbjj.** Title 32, USC, *National Guard.*
- **eemm.** Unified Command Plan 2002 with changes.

2. Department Of Defense

  
  
  
  d. DODD 3020.XX, *Critical Infrastructure Protection Program. (Draft)*
  
  
  
  g. DODD 3025.12, *Military Assistance for Civil Disturbances, 4 February 1994.*
  
  h. DODD 3025.15, *Military Assistance to Civil Authorities, 18 February 1997.*
  
  
  
  k. DODD 5100.1, *Functions of Department of the Defense and Its Major Components, 1 August 2002.*


5. DOD Instruction 3020, Implementation of the Critical Infrastructure Program. (Draft)


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 1-01, Joint Publication System, Joint Doctrine and Joint Tactics, Techniques and Procedures Development Program.

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


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

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

h. JP 3-0, Doctrine for Joint Operations.

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

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


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

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


r. JP 3-14, *Joint Doctrine for Space Operations.*


u. JP 3-33, *Joint Force Capabilities.*


w. JP 3-52, *Doctrine for Joint Airspace Control in the Combat Zone.*


z. JP 3-56.1, *Command and Control of Joint Air Operations.*


bb. JP 4-0, *Doctrine for Logistics Support of Joint Operations.*

cc. JP 4-02, *Doctrine for Health Service Support in Joint Operations.*

dd. JP 4-04, *Joint Doctrine for Civil Engineering Support.*

ee. JP 5-0, *Doctrine for Planning Joint Operations.*

ff. JP 5-00.1, *Joint Doctrine for Campaign Planning.*

Appendix C


2. ii. Joint Military [Operations](#) Historical Collection


4. kk. Chairman of the Joint Chiefs of Staff Instruction, (CJCSI) 3110.01, *Joint Strategic Capabilities Plan (JSCP)*, 1 October 2002.


8. oo. 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.

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


13. tt. CJCSI 5113.02A, *Chairman of the Joint Chiefs of Staff Counterproliferation Charter (U)*, 10 August 2000, document is classified secret (S).

14. uu. CJCSI 8510.01, *Joint Modeling and Simulation Management*.

4. Army Publications


c. FM 3-100.4, *Environmental Considerations in Military Operations*.


5. **Navy Publications**


4. **Marine Corps Publications**


   b.—Marine Corps Reference Publication 4-11B, *Environment Considerations in Military Operations*.

5. **Air Force Publications**


6. **Coast Guard Publications**

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

Intentionally Blank
APPENDIX F
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication to: Commander, United States Joint Forces Command, Joint Warfighting Center, Code JW100, 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 the Army. 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-JTED//

   Routine changes should be submitted to the Director for Operational Plans and Interoperability (J-7), JDETD, 7000 Joint Staff Pentagon, Washington, D.C. 20318-7000 with info copies to USJFCOM JWFC.

   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

<table>
<thead>
<tr>
<th>CHANGE</th>
<th>COPY</th>
<th>DATE OF</th>
<th>DATE</th>
<th>POSTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>NUMBER</td>
<td>CHANGE</td>
<td>ENTERED</td>
<td>REMARKS</td>
</tr>
</tbody>
</table>

4. Distribution

a. Copies of this publication can be obtained in CD format for initial distribution through the Service publication centers listed below or electronically through the Joint Electronic Library (http://www.dtic.mil/doctrine/).
b. Only approved pubs and test pubs 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, Pentagon, Washington D.C. 20301-7400.


Army: US Army AG Publication Center  
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: Marine Corps Logistics Base  
Albany, GA  31704-5000  

USJFCOM 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.
### Glossary

#### Part I — Abbreviations and Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADS</td>
<td>advanced distributive simulation</td>
</tr>
<tr>
<td>AOR</td>
<td>area of responsibility</td>
</tr>
<tr>
<td>ARC</td>
<td>American Red Cross</td>
</tr>
<tr>
<td>ASD(HD)</td>
<td>Assistant Secretary of Defense for Homeland Defense</td>
</tr>
<tr>
<td>ASD(RA)</td>
<td>Assistant Secretary of Defense for Reserve Affairs</td>
</tr>
<tr>
<td>ASD(SO/LIC)</td>
<td>Assistant Secretary of Defense for Special Operations and Low Intensity Conflict</td>
</tr>
<tr>
<td>AT</td>
<td>antiterrorism</td>
</tr>
<tr>
<td>BMD</td>
<td>ballistic missile defense</td>
</tr>
<tr>
<td>BTS</td>
<td>Border and Transportation Security</td>
</tr>
<tr>
<td>C2</td>
<td>command and control</td>
</tr>
<tr>
<td>C4I</td>
<td>command, control, communications, computers, and intelligence</td>
</tr>
<tr>
<td>CATS</td>
<td>consequence assessment tool set</td>
</tr>
<tr>
<td>CBRNE</td>
<td>chemical, biological, radiological, nuclear, and high-yield explosive</td>
</tr>
<tr>
<td>CD</td>
<td>counterdrug</td>
</tr>
<tr>
<td>CDRUSJFCOM</td>
<td>Commander, US Joint Forces Command</td>
</tr>
<tr>
<td>CDRNORAD</td>
<td>Commander, North American Air Defense Command</td>
</tr>
<tr>
<td>CDRUSNORTHCOM</td>
<td>Commander, US Northern Command</td>
</tr>
<tr>
<td>CDRUSPACOM</td>
<td>Commander, US Pacific Command</td>
</tr>
<tr>
<td>CDRUSSOCOM</td>
<td>Commander, US Special Operations Command</td>
</tr>
<tr>
<td>CDRUSSOUTHCOM</td>
<td>Commander, US Southern Command</td>
</tr>
<tr>
<td>CDRUSTRATCOM</td>
<td>Commander, US Strategic Command</td>
</tr>
<tr>
<td>CDRUSTRANSCOM</td>
<td>Commander, US Transportation Command</td>
</tr>
<tr>
<td>CI</td>
<td>counterintelligence</td>
</tr>
<tr>
<td>CIA</td>
<td>Central Intelligence Agency</td>
</tr>
<tr>
<td>CIP</td>
<td>critical infrastructure protection</td>
</tr>
<tr>
<td>CJCSC</td>
<td>Chairman, Joint Chiefs of Staff</td>
</tr>
<tr>
<td>CJSICSI</td>
<td>Chairman of the Joint Chiefs of Staff instruction</td>
</tr>
<tr>
<td>CM</td>
<td>consequence management</td>
</tr>
<tr>
<td>CMOC</td>
<td>Cheyenne Mountain Operations Center</td>
</tr>
<tr>
<td>CNGB</td>
<td>Chief, National Guard Bureau</td>
</tr>
<tr>
<td>CNO</td>
<td>computer network operations</td>
</tr>
<tr>
<td>COCOM</td>
<td>combatant command (command authority)</td>
</tr>
<tr>
<td>COG</td>
<td>continuity of government</td>
</tr>
<tr>
<td>CONPLAN</td>
<td>concept plan</td>
</tr>
<tr>
<td>CONUS</td>
<td>continental United States</td>
</tr>
<tr>
<td>COOP</td>
<td>continuity of operations</td>
</tr>
<tr>
<td>COP</td>
<td>common operational picture</td>
</tr>
<tr>
<td>CPG</td>
<td>Contingency Planning Guidance</td>
</tr>
<tr>
<td>CrM</td>
<td>crisis management</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Glossary</strong></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>CS</td>
</tr>
<tr>
<td>2</td>
<td>CST</td>
</tr>
<tr>
<td>3</td>
<td>DCI</td>
</tr>
<tr>
<td>4</td>
<td>DCIP</td>
</tr>
<tr>
<td>5</td>
<td>DCO</td>
</tr>
<tr>
<td>6</td>
<td>DEST</td>
</tr>
<tr>
<td>7</td>
<td>DHS</td>
</tr>
<tr>
<td>8</td>
<td>DNWS</td>
</tr>
<tr>
<td>9</td>
<td>DOD</td>
</tr>
<tr>
<td>10</td>
<td>DODD</td>
</tr>
<tr>
<td>11</td>
<td>DOE</td>
</tr>
<tr>
<td>12</td>
<td>DOJ</td>
</tr>
<tr>
<td>13</td>
<td>DOS</td>
</tr>
<tr>
<td>14</td>
<td>DOT</td>
</tr>
<tr>
<td>15</td>
<td>DTRA</td>
</tr>
<tr>
<td>16</td>
<td>EO</td>
</tr>
<tr>
<td>17</td>
<td>EPA</td>
</tr>
<tr>
<td>18</td>
<td>ESF</td>
</tr>
<tr>
<td>19</td>
<td>EXECSEC</td>
</tr>
<tr>
<td>20</td>
<td>FBI</td>
</tr>
<tr>
<td>21</td>
<td>FCO</td>
</tr>
<tr>
<td>22</td>
<td>FEMA</td>
</tr>
<tr>
<td>23</td>
<td>FI</td>
</tr>
<tr>
<td>24</td>
<td>FP</td>
</tr>
<tr>
<td>25</td>
<td>FRERP</td>
</tr>
<tr>
<td>26</td>
<td>FRP</td>
</tr>
<tr>
<td>27</td>
<td>GSA</td>
</tr>
<tr>
<td>28</td>
<td>HLD</td>
</tr>
<tr>
<td>29</td>
<td>HLS</td>
</tr>
<tr>
<td>30</td>
<td>HPAC</td>
</tr>
<tr>
<td>31</td>
<td>HSC</td>
</tr>
<tr>
<td>32</td>
<td>HSPD</td>
</tr>
<tr>
<td>33</td>
<td>IA</td>
</tr>
<tr>
<td>34</td>
<td>INRP</td>
</tr>
<tr>
<td>35</td>
<td>IO</td>
</tr>
<tr>
<td>36</td>
<td>ISR</td>
</tr>
<tr>
<td>1</td>
<td>JA</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>2</td>
<td>JDOMS</td>
</tr>
<tr>
<td>3</td>
<td>JFC</td>
</tr>
<tr>
<td>4</td>
<td>JOC</td>
</tr>
<tr>
<td>5</td>
<td>JP</td>
</tr>
<tr>
<td>6</td>
<td>JTF</td>
</tr>
<tr>
<td>7</td>
<td>JTF-CS</td>
</tr>
<tr>
<td>8</td>
<td>LEA</td>
</tr>
<tr>
<td>9</td>
<td>LFA</td>
</tr>
<tr>
<td>10</td>
<td>LEA</td>
</tr>
<tr>
<td>11</td>
<td>MACA</td>
</tr>
<tr>
<td>12</td>
<td>MACDIS</td>
</tr>
<tr>
<td>13</td>
<td>M&amp;S</td>
</tr>
<tr>
<td>14</td>
<td>MI</td>
</tr>
<tr>
<td>15</td>
<td>MOA</td>
</tr>
<tr>
<td>16</td>
<td>MOU</td>
</tr>
<tr>
<td>17</td>
<td>MSCA</td>
</tr>
<tr>
<td>18</td>
<td>MSCLEA</td>
</tr>
<tr>
<td>19</td>
<td>NCI/KA</td>
</tr>
<tr>
<td>20</td>
<td>NG</td>
</tr>
<tr>
<td>21</td>
<td>NGB</td>
</tr>
<tr>
<td>22</td>
<td>NMS</td>
</tr>
<tr>
<td>23</td>
<td>NSHS</td>
</tr>
<tr>
<td>24</td>
<td>NSPD</td>
</tr>
<tr>
<td>25</td>
<td>NSS</td>
</tr>
<tr>
<td>26</td>
<td>NORAD</td>
</tr>
<tr>
<td>27</td>
<td>NRPA</td>
</tr>
<tr>
<td>28</td>
<td>NSA</td>
</tr>
<tr>
<td>29</td>
<td>NSC</td>
</tr>
<tr>
<td>30</td>
<td>NSS</td>
</tr>
<tr>
<td>31</td>
<td>NSSE</td>
</tr>
<tr>
<td>32</td>
<td>OPCON</td>
</tr>
<tr>
<td>33</td>
<td>OPSEC</td>
</tr>
<tr>
<td>34</td>
<td>OSD</td>
</tr>
<tr>
<td>35</td>
<td>PA</td>
</tr>
<tr>
<td>36</td>
<td>PAG</td>
</tr>
<tr>
<td>37</td>
<td>PAO</td>
</tr>
<tr>
<td>38</td>
<td>PCA</td>
</tr>
<tr>
<td>39</td>
<td>PCC</td>
</tr>
<tr>
<td>40</td>
<td>PDD</td>
</tr>
<tr>
<td>41</td>
<td>PHSAC</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>POD</td>
<td>port of debarkation</td>
</tr>
<tr>
<td>POE</td>
<td>port of embarkation</td>
</tr>
<tr>
<td>PSYOP</td>
<td>psychological operations</td>
</tr>
<tr>
<td>RC</td>
<td>Reserve Component</td>
</tr>
<tr>
<td>RFA</td>
<td>request for assistance</td>
</tr>
<tr>
<td>ROE</td>
<td>rules of engagement</td>
</tr>
<tr>
<td>RUF</td>
<td>rules for the use of force</td>
</tr>
<tr>
<td>SecDef</td>
<td>Secretary of Defense</td>
</tr>
<tr>
<td>SECNAV</td>
<td>Secretary of the Navy</td>
</tr>
<tr>
<td>SJFHQ-N</td>
<td>Standing Joint Force Headquarters-North</td>
</tr>
<tr>
<td>SJFHQ-NCR</td>
<td>Standing Joint Force Headquarters-National Capital Region</td>
</tr>
<tr>
<td>SPG</td>
<td>strategic planning guidance</td>
</tr>
<tr>
<td>SROE</td>
<td>standing rules of engagement</td>
</tr>
<tr>
<td>SS</td>
<td>Secret Service</td>
</tr>
<tr>
<td>TREAS</td>
<td>Department of the Treasury</td>
</tr>
<tr>
<td>UAV</td>
<td>unmanned aerial vehicle</td>
</tr>
<tr>
<td>UCP</td>
<td>Unified Command Plan</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
</tr>
<tr>
<td>USAFR</td>
<td>United States Air Force Reserve</td>
</tr>
<tr>
<td>USAR</td>
<td>United States Army Reserve</td>
</tr>
<tr>
<td>USC</td>
<td>United States Code</td>
</tr>
<tr>
<td>USCG</td>
<td>United States Coast Guard</td>
</tr>
<tr>
<td>USCGR</td>
<td>United States Coast Guard Reserve</td>
</tr>
<tr>
<td>USNORTHCOM</td>
<td>United States Northern Command</td>
</tr>
<tr>
<td>USPACOM</td>
<td>United States Pacific Command</td>
</tr>
<tr>
<td>USSTRATCOM</td>
<td>United States Strategic Command</td>
</tr>
<tr>
<td>WMD</td>
<td>weapons of mass destruction</td>
</tr>
<tr>
<td>WMD-CST</td>
<td>weapons of mass destruction-combat support team</td>
</tr>
</tbody>
</table>
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)

air and missile defense. The integration of joint force capabilities to deter, preempt, defend against and destroy adversary aircraft and missiles, both before and after launch. Also called AMD. (Upon approval of this publication, this term and its definition will be included in 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)

attack operations. Offensive actions intended to disrupt or destroy adversary threats and capabilities before, during, and after an attack. (Upon approval of this publication, this term and its definition will be included in JP 1-02.)

catastrophic disaster response group. A group of representatives at the national level from the Federal departments and agencies that have Federal response plan support responsibilities. Also called the CDRG. (Upon approval of this publication, this term and its definition will be included in JP 1-02.)

chemical, biological, radiological, nuclear, or high yield explosive incidents. Emergencies resulting from the deliberate or unintentional use of a WMD, 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. (Upon approval of this publication, this term and its definition will modify the existing term and its definition and will be included in 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. (Upon approval of this publication, this term and its definition will modify the existing term “United States Civil Authorities” and will be included in JP 1-02 and will replace the term United States Civil Authorities.)

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
civil defense emergency. See domestic emergencies.

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

civil disturbance readiness conditions. Required conditions of preparedness to be attained by military forces in preparation for deployment to an objective area in response to an actual or threatened civil disturbance. (JP 1-02)

civil-military operations. The activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area in order to facilitate military operations, to consolidate and achieve operational US objectives. Civil-military operations may include performance by military forces of activities and functions normally the responsibility of the local, regional, or national government. These activities may occur prior to, during, or subsequent to other military actions. They may also occur, if directed, in the absence of other military operations. Civil-military operations may be performed by designated civil affairs, by other military forces, or by a combination of civil affairs and other forces. Also called CMO. (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. (Upon approval of this publication, this term and its definition will be included in 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)

consequence management. Actions taken that comprise those essential services and activities required to maintain or restore essential services and manage and mitigate problems resulting from disasters and catastrophes, including natural, manmade, or terrorist incidents. Such services may include transportation, communications, public works and engineering, fire fighting, information planning, mass care, resources support, health and medical services, urban search and rescue, hazardous materials, food, and energy. Also called CM. (Upon approval of this publication, this term and its definition will modify the existing term and its definition and will be included in 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)

counterterrorism. Offensive measures taken to prevent, deter, and respond to terrorism. Also called CT. See also antiterrorism; combating terrorism; terrorism. (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. (Upon approval of this publication, this term and its definition will be included in JP 1-02.)

critical asset assurance. A process of identifying assets deemed critical to the Department of Defense, assessing the potential threats, quantifying the impact of non-availability, identifying potential restoration actions to restore lost, damaged, corrupted, or compromised assets, and identifying and recommending options to protect, mitigate, and improve availability. Also called CAA. (Upon approval of this publication, this term and its definition will be included in JP 1-02.)

critical infrastructure. Designated capabilities, facilities and systems considered essential to the maintenance of the stability and good order of a nation. See also defense critical infrastructure and national critical infrastructure and key assets. (Upon approval of this publication, this term and its definition will be included in JP 1-02.)

critical infrastructure protection. The identification, assessment, and security enhancement of physical and cyber-assets and associated infrastructures essential to the execution of the National Military Strategy, orderly functioning of the government, economy, domestic activities and for the mobilization, deployment, employment, sustainment, and redeployment of US military operations. It links mission assurance aspects of antiterrorism, force protection, information assurance, continuity of operations, and readiness programs. Also called CIP. See also defense critical infrastructure and national critical infrastructure. (Upon approval of this publication, this term and its definition will be included in JP 1-02.)

危机管理。用于识别、获取、计划使用资源以预见、预防、和/或解决威胁或恐怖主义事件。它通常是执法部门的响应，通常由联邦法律执行。也称为CrM。 ( Upon approval of this publication, this term and its definition will be included in JP 1-02.)

Department of Defense installation. A facility subject to the custody, jurisdiction, or
administration of any DOD Department of Defense component. This term includes, but is not limited to, military reservations, installations, bases, posts, camps, stations, arsenals, vessel/ship, or laboratories where a DOD Department of Defense component has operational responsibility for facility security and defense. (Upon approval of this publication, this term and its definition will be included in JP 1-02.)

defense coordinating officer. A military or civilian official of any Department of Defense component, who has been designated by the DOD Department of Defense executive agent or responsible DOD component to exercise some delegated authority of the DOD Department of Defense executive agent to coordinate military support to civil authorities activities. Also called DCO. (Upon approval of this publication, this term and its definition will be included in JP 1-02.)

defense critical infrastructure. Designated capabilities, facilities, and systems considered critical for DOD to execute the national military strategy. This infrastructure can be owned by DOD, or exist in the commercial or other government sectors—DOD and non-DOD assets and associated infrastructure essential to project and support military forces worldwide. Also called DCI. (Upon approval of this publication, this term and its definition will be included in JP 1-02.)

defense industrial base. The worldwide organic and private sector industrial complex with capabilities to design, produce, and maintain military weapons systems, subsystem, components, parts, or provide other goods and services to meet military requirements. Also called DIB. (Upon approval of this publication, this term and its definition will be included in JP 1-02.)

defense sectors. An identified grouping of Department of Defense functions that perform essential services required for warfighter operations and their ability to project and support forces worldwide. (Upon approval of this publication, this term and its definition will be included in 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 emergency” includes any or all of the emergency conditions defined below: a. civil defense emergencies. 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 Chapter 15 of Title 10 USC 15—United States Code. 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 United States Code
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. (Upon approval of this publication, this term and its
definition will modify the existing term and its definition and will be included in JP
1-02)

“domestic support operations. Those activities and measures taken by the Department
of Defense to foster mutual assistance and support between the Department of
Defense and any civil government agency in planning or preparedness for, or in the
application of resources for response to, the consequences of civil emergencies or
attacks, including national security emergencies.

emergency preparedness. Measures taken in advance of an emergency to reduce the
loss of life and property and to protect the Nation’s institutions from all
types of hazards through a comprehensive emergency management program of
preparedness, mitigation, response, and recovery. (Upon approval of this
publication, this term and its definition will be included in JP 1-02.)

emergency preparedness liaison officer. A senior Reserve officer who is a
representative of the Service Planning Agent, the Federal Emergency Management
Agency, and a designated Defense Coordinating Officer. Also called EPLO. (Upon
approval of this publication, this term and its definition will be included in JP 1-02.)

emergency support function. A functional area of response activity established to
facilitate coordinated federal delivery of assistance required during the immediate
response phase after a major disaster or civil emergency to save lives, protect
property and public health, and maintain public safety. Also called ESF. (Upon
approval of this publication, this term and its definition will be included in 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. (Upon approval of this
publication, this term and its definition will modify the existing term and its
definition and will be included in 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. An agreement between equals does not create an executive agent. For example, a Service cannot become a Department of Defense executive agent for a particular matter with simply the agreement of the other Services; such authority must be delegated by the Secretary of Defense. 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. See also planning agent. (Upon approval of this publication, this term and its definition will modify the existing term and its definition and will be included in JP 1-02.)

federal coordinating officer. Appointed by the Director of the Federal Emergency Management Agency, on behalf of the President, to coordinate federal assistance to a state affected by a disaster or emergency. The source and level of the federal coordinating officer will likely depend on the nature of the federal response. Also called FCO. (JP 1-02)

Federal Response Plan. The inter-departmental planning mechanism, developed under Federal Emergency Management Agency—Department of Homeland Security leadership, by which the Federal government prepares for and responds to the consequences of catastrophic or major disasters and emergencies. Note: This plan will be incorporated into the National Response Plan. Also called FRP. (Upon approval of this publication, this term and its definition will be included in 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)

global strike. Rapidly planned, limited duration extended range precision attacks directed against highly valued adversary assets. (This term and its definition are provided for information and are proposed for inclusion in the next edition of JP 1-02 by JP 3-70.)

homeland. The physical region that includes the continental United States, Alaska, and Hawaii, United States territories, possessions, and surrounding territorial waters and airspace. (Upon approval of this publication, this term and its definition will be included in JP 1-02.)
**homeland defense.** The protection of United States territory, sovereignty, domestic population, and critical infrastructure against external threats and aggression. Also called HL-D. (Upon approval of this publication, this term and its definition will be included in 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. (Upon approval of this publication, this term and its definition will be included in JP 1-02.)

**incident management.** A single 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 national level. (Upon approval of this publication, this term and its definition will be included in 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)

**immediate response.** Any form of immediate action taken by a Department of Defense component or military commander, under the authority of DOD Directive 3025.1, to assist civil authorities or the public to save lives, prevent human suffering, or mitigate great property damage under imminently serious conditions and when time does not permit approval from a higher authority. (Upon approval of this publication, this term and its definition will be included in 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. (Upon approval of this publication, this term and its definition will replace the term “elements of national power” and be included in 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 movement center.** The center established to coordinate the employment of all means of transportation (including those provided by allies or host nations) to support the concept of operations. This coordination is accomplished through establishment of transportation policies within the assigned operational area, consistent with the relative urgency of need, port and terminal capabilities, transportation asset availability, and priorities set by a joint force commander. Also called JMC. (Upon approval of this publication, this term and its definition will modify the existing term and its definition and will be included in JP 1-02.)

**joint regional defense command.** A joint task force headquarters formed on order of the Commander in Chief, United States Atlantic Command within designated continental United States (CONUS) multistate regions, to command and control (1) execution of land defense of CONUS; and (2) military assistance to civil authority missions.

**joint state area command.** A joint task force headquarters formed on order of Commander in Chief, United States Atlantic Command, within existing state boundaries to command and control United States and federalized state elements designated to execute land defense of the continental United States, military support to civil defense, and military assistance to civil authority missions. (Upon approval of this publication, this term and its definition will be removed from 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 is referred to as the Lead Federal Agency and is determined by the type of emergency. Specific responsibilities of a Lead Federal Agency vary according to the agency’s unique statutory authorities. Also called LFA. (Upon approval of this publication, this term and its definition will be included in JP 1-02.)

**major disaster.** See domestic emergencies.

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

**military assistance to civil authorities.** A mission set of civil support following natural or manmade disasters, chemical, biological, radiological, nuclear, or high explosive consequence management, and other support as required—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. (Upon approval of this publication, this term and its definition will be included in JP 1-02.)

**military assistance to civil disturbances.** A mission set of civil support involving DOD 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. (Upon approval of this publication, this term and definition will appear in JP 1-02.)

**military support to civil authorities.** A mission of civil support consistent of support for natural or manmade disasters and chemical, biological, radiological, nuclear, or high yield explosive consequence management, and other support as required. Also called MSCA. (Upon approval of this publication, this term and its definition will be included in JP 1-02.)

**military support to civilian law enforcement agencies.** A mission set of DOD support military assistance to civil authorities that includes support to civilian law enforcement agencies. This includes but is not limited to: combating terrorism, counterdrug operations, national security special events, border patrol augmentation, and national critical infrastructure and key asset protection. Also called MSCLEA. (Upon approval of this publication, this term and definition will appear in JP 1-02.)

**mitigation.** The process of reducing or minimizing the adverse impact of incidents through pre-planned and coordinated reactions. This process supports crisis management response and facilitates reconstitution. (Upon approval of this publication, this term and its definition will be included in JP 1-02.)

**national critical infrastructure and key assets.** Those infrastructures essential to the functioning of the nation and whose incapacity or destruction would have a debilitating regional or national impact. They include telecommunications, electrical power systems, gas and oil transportation and storage, water supply systems, banking and finance, transportation, emergency services, industrial assets, information systems, and continuity of government operations. The infrastructure and assets vital to our national security, governance, public health and safety, economy, and public confidence. They include telecommunications, electrical power systems, gas and oil transportation and storage, water supply systems, banking and finance, transportation, emergency services, industrial assets, information systems, and continuity of government operations. Also called NCI/KA. (Upon approval of this...
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)

national security emergency. Any occurrence, including natural disaster, military attack, technological emergency, or other emergency, that seriously degrades or threatens the national security of the United States. (Upon approval of this publication, this term and its definition will be included in JP 1-02.)

planning agent. A military or civilian official of any Department of Defense component who has been designated by the head of that component to exercise delegated authority—responsibility for civil assistance—support planning for the entire component or for certain subordinate elements or a specified geographic area. See also executive agent. (Upon approval of this publication, this term and its definition will be included in JP 1-02.)

primary agency. The federal department or agency assigned primary responsibility for managing and coordinating a specific emergency support function in the Federal Response Plan. (Upon approval of this publication, this term and its definition will be included in JP 1-02.)

principal 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. Also called PPA. (Upon approval of this publication, this term and its definition will be included in JP 1-02.)

radiological accident. A loss of control over radiation or radioactive material that presents a hazard to life, health, or property or that may result in any member of the general population exceeding exposure limits for ionizing radiation. (Upon approval of this publication, this term and its definition will be included in JP 1-02.)

response task force. A Department of Defense response force appropriately manned, equipped, trained and able to perform and coordinate all actions necessary to control and recover from a radiological accident or significant incident. Also called RTF. (Upon approval of this publication, this term and its definition will be included in JP 1-02.)

rules for the use of force. Directives issued to guide United States forces on the use of force during civil support operations. These directives may take the form of mission execute orders, deployment orders, memoranda of agreement, or plans. Also called RUF. (Upon approval of this publication, this term and its definition will be included in JP 1-02.)
rules of engagement. Directives issued by competent military authority that delineates
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. All defensive measures designed to destroy attacking enemy vehicles
(including missiles) while in space, or to nullify or reduce the effectiveness of such
attack. See also aerospace defense. (Upon approval of this publication, this term
and definition will be removed from JP 1-02.)

state coordinating officer. The person appointed by the governor to coordinate state and
local response efforts with those of the Federal Government. Also called SCO.
(Upon approval of this publication, this term and its definition will be included in 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. (Upon approval of this publication, this
term and its definition will be included in 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)

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. (Upon approval of this
publication, this term and its definition will be included in JP 1-02) (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.)
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:

**STEP #1**
**Project Proposal**
- Submitted by Services, combatant commands, or Joint Staff to fill extant operational void
- J-7 validates requirement with Services and combatant commands
- J-7 initiates Program Directive

**STEP #2**
**Program Directive**
- J-7 formally staffs with Services and combatant commands
- Includes scope of project, references, milestones, and who will develop drafts
- J-7 releases Program Directive to Lead Agent. Lead Agent can be Service, combatant command, or Joint Staff (JS) Directorate

**STEP #3**
**Two Drafts**
- Lead Agent selects Primary Review Authority (PRA) to develop the pub
- PRA develops two draft pubs
- PRA staffs each draft with combatant commands, Services, and Joint Staff

**STEP #4**
**CJCS Approval**
- Lead Agent forwards proposed pub to Joint Staff
- Joint Staff takes responsibility for pub, makes required changes and prepares pub for coordination with Services and combatant commands
- Joint Staff conducts formal staffing for approval as a JP

**STEP #5**
**Assessments/Revision**
- The combatant commands receive the JP and begin to assess it during use
- 18 to 24 months following publication, the Director, J-7, will solicit a written report from the combatant commands and Services on the utility and quality of each JP and the need for any urgent changes or earlier-than-scheduled revisions
- No later than 5 years after development, each JP is revised

**ENHANCED JOINT WARFIGHTING CAPABILITY**

*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:*