DCSINT Handbook No. 1.04

Defense Support of Civil Authorities

US Army Training and Doctrine Command
Deputy Chief of Staff for Intelligence
Assistant Deputy Chief of Staff for Intelligence - Threats
Fort Leavenworth, Kansas

15 August 2005

This Page Intentionally Blank

Preface

Defense Support to Civil Authorities: WMD/E Consequence Management is a supplemental handbook that presents an appreciation of U.S. military forces and their roles as part of Department of Defense support to Federal emergency response in a terrorist WMD/E incident. This handbook supports a U.S. Army Training and Doctrine Command, Deputy Chief of Staff for Intelligence capstone reference guide on terrorism, DCSINT Handbook No. 1, ***A Military Guide to Terrorism in the Twenty-First Century***. Both the capstone guide and supplemental handbook are prepared under the direction of the U.S. Army Training and Doctrine Command, Assistant Deputy Chief of Staff for Intelligence-Threats. Understanding WMD/E and terrorism spans foreign and domestic threats with specific strategies, tactics, and targets. A central aspect of this handbook comprises is the use of U.S. military capabilities during a chemical, biological, radiological, nuclear, or high yield explosive (CBRNE) incident in a contemporary operational environment (COE).

Purpose. This informational handbook supports operational missions, institutional training, and professional military education for U.S. military forces in the Global War on Terrorism (GWOT) and Defense Support of Civil Authorities (DSCA). This document promotes an improved understanding of terrorist objectives, motivation, and intention to use WMD/E; and accent probable missions of U.S. military forces in WMD/E incident response. Compiled from open source materials, this handbook promotes a "Threats" perspective and enemy situational awareness of U.S. actions in combating terrorism.

Intended Audience. This handbook exists primarily for U.S. military forces, and invites a common situational awareness in the context of forces that may be deployed in support of Federal response to a WMD/E incident. Other applicable groups may include interdepartmental, interagency, intergovernmental, civilian contractor, non-governmental, private volunteer, humanitarian relief organizations, and the general citizenry.

Handbook Use. Study of contemporary terrorist behavior and motivation, terrorist goals and objectives, and a composite of probable terrorist tactics, techniques, and procedures (TTP) improves readiness of U.S. military forces. As a living document, this handbook will be updated as necessary to ensure a current and relevant resource. A selected bibliography presents citations for detailed study of specific terrorism topics. Unless stated otherwise, masculine nouns or pronouns do not refer exclusively to men.

Proponent Statement. Headquarters, U.S. Army Training and Doctrine Command (TRADOC) is the proponent for this publication. Periodic updates will accommodate emergent user requirements on terrorism. Send comments and recommendations on DA Form 2028 directly to TRADOC Assistant Deputy Chief of Staff for Intelligence – Threats at the following address: Director, TRADOC ADCSINT – Threats, ATTN: ATIN-L-T (Bldg 53), 700 Scott Avenue, Fort Leavenworth, Kansas 66027-1323. This handbook is available at Army Knowledge Online (**www.us.army.mil**). Additionally, the General Dennis J. Reimer Training and Doctrine Digital Library (www.adtdl.army.mil) lists the handbook as a special text.

This Page Intentionally Blank

ACKNOWLEDGEMENTS
Threats Terrorism Team (T3) Network

The Deputy Chief of Staff for Intelligence at U.S. Army Training and Doctrine Command extends special appreciation to the many stakeholders who were invited to contribute information, subject matter expertise, and insight into the update of this 2005 unclassified terrorism handbook, *A Military Guide to Terrorism in the Twenty-First Century.*

This expanding partnership of the Threats Terrorism Team (T3) Network in conjunction with the Assistant Deputy Chief of Staff for Intelligence-Threats includes:

U.S. Northern Command, J2 Combined Intelligence and Fusion Center (CIFC)
U.S. Northern Command, Director of Operations, J3
U.S. Northern Command, J34, Force Protection and Risk Management Branch
U.S. Northern Command, J35
U.S. Northern Command, JTF-Civil Support, J5 Plans, CBRNE Consequence Management
U.S. European Command, Plans and Operations Center
U.S. Pacific Command, Antiterrorism and Training Branch, J34
U.S. Pacific Command, U.S. Marine Forces Pacific, G5
U.S. Central Command, J2
U.S. Special Operations Command, Center for Special Operations, J23
U.S. Southern Command, J2
U.S. Strategic Command, Joint Intelligence Center, J2201
U.S. Joint Forces Command, J9
U.S. Joint Forces Command, J34
Joint Staff, J34 Deputy Directorate for Antiterrorism/Homeland Defense
Joint Staff, J5 War on Terrorism Directorate, Strategic Planning Division
Joint Military Intelligence Training Center (JMITC)
State Department, Bureau of Diplomatic Security, Intelligence-Threats Analysis Directorate
Office of the Assistant Secretary of Defense for Homeland Defense
Department of Energy, Office of Headquarters Security Operations
Department of Homeland Security, Director Preparedness Division, Operational Integration Staff
Department of Homeland Security, Federal Emergency Management Agency, Region VII
Department of Homeland Security, Citizen Corps FEMA Region VII Program Manager
Department of Homeland Security, Transportation Security Administration, KCI Airport
Federal Bureau of Investigation (FBI) Terrorism Watch and Warning Unit
FBI, National Joint Terrorism Task Force (NJTTF)
FBI, Counterterrorism Division, Military Liaison and Detainee Unit
U.S. First Army Headquarters, Military Support Division, G3
U.S. Fifth Army Headquarters, G3
U.S. Navy Center for Antiterrorism and Navy Security Forces
U.S. Navy, Naval War College
U.S. Navy, Navy Command and Staff College
U.S. Marine Corps Training and Education Command, G3 Training Readiness, Plans and Policy
U.S. Marine Corps, Marine War College
U.S. Marine Corps, Marine Corps Command and Staff College
U.S. Air Force Security Forces Center
U.S. Air Force, National Air and Space Intelligence Center, Behavioral Influences Analysis Division
U.S. Air Force, Air War College
U.S. Air Force, Air Command and Staff College
U.S. Army Office of Deputy Chief of Staff G2, for Counterintelligence, HUMINT, and Security

U.S. Army Office of the Chief Information Officer (CIO)/G6
U.S. Army Network Enterprise Technology Command, 9th ASC, G2
U.S. Army Network Enterprise Technology Command, Office of Information Assurance
U.S. Military Academy (West Point), Combating Terrorism Center (CTC)
U.S. Army Combined Arms Center (CAC)
U.S. Army Maneuver Support Center (MANSCEN)
U.S. Army Combined Arms Support Command (CASCOM)
U.S. Army Combined Arms Center-Training (CAC-T)
U.S. Army Battle Command Training Program (BCTP)
National Defense University
U.S. Army TRADOC Centers and Schools, including:
U.S. Army, Army War College
U.S. Army Command and General Staff College (CGSC)
U.S. Army Logistics Management College (ALMC)
U.S. Army Aviation Logistics Center
U.S. Army Management Staff College
U.S. Army School of Information Technology
U.S. Army Leader College for Information Technology
U.S. Army Fort Eustis, Directorate of Plans, Training, Mobilization, and Security
U.S. Army Command and General Staff School (CGSS)
U.S. Army School for Command Preparation (SCP)
U.S. Army School for Advanced Military Studies (SAMS)
U.S. Army Center for Army Leadership (CAL)
U.S. Army Infantry Center, G2 Director of Intelligence and Security
U.S. Army Intelligence Center, Futures Development and Integration Center
U.S. Army Warrant Officer Career Center
U.S. Army Sergeants Major Academy
U.S. Army Soldier Support Institute
U.S. Army Academy of Health Sciences, Medical Department Center and School
U.S. Army Nuclear and Chemical Agency
U.S. Northern Command, Homeland Security/Defense Education Consortium (HSDEC)
U.S. Army TRADOC, Assistant Deputy Chief of Staff for Intelligence-Threats

Defense Support to Civil Authorities

Contents

Introduction

Defense Support to Civil Authorities is a supplemental handbook to the U.S. Army TRADOC DCSINT Handbook No.1, ***A Military Guide to Terrorism in the Twenty-First Century,*** as a capstone reference guide that describes terrorism[1] and its potential impact on U.S. military forces in the conduct of mission operations. This supplemental handbook highlights the nature of terrorism present in a full spectrum contemporary operational environment (COE),[2] and the likely impacts on U.S. military operations related to consequence management support in a WMD/E incident. Terrorism and terrorist intent to obtain and use weapons of mass destruction or effect is one of the most serious threats to our Nation.

Despite the consistent menace, terrorism is a threat that is poorly understood, and frequently confused due to widely divergent views over exactly what defines terrorism. Terrorism, as discussed in this handbook, centers on known principal terrorist "Threats" to the United States of America. The United States confronts terrorism in daily circumstances, both foreign and domestic; and prepares for security against terrorism expected in the foreseeable future. The most significant U.S. concerns are terrorist organizations with demonstrated global reach capabilities and those terrorist organizations that seek to acquire and use weapons of mass destruction (WMD). Nonetheless, the threat of terrorism to the U.S. is present across the entire spectrum of conflict. The use of terrorism ranges from individual acts of wanton damage or destruction to property or person, to highly sophisticated operations conducted by highly organized violent groups with social, environmental, religious, economic, or political agendas. This full range of terrorist activity can have significant negative impact on the conduct of missions by U.S. military forces.

Purpose

This handbook serves as an unclassified resource to inform U.S. military members on the nature and characteristics of terrorism. The intention is to create situational awareness and understanding of current terrorism capabilities and limitations, and complement the deliberate processes of military risk management, force protection, and mission orders conduct and leader decision-making.

From a "Threats" perspective, terrorism *capabilities and limitations* indicate possible and probable types of threat action that may be directed against U.S. military members, units, and organizations. Factors other than military power may place *constraints* on both threats and friendly forces. Commanders, organizational leaders, and other military members can "think like the threat" and use this handbook to create operational *opportunities* to:

---

[1] Joint Publication 1-02. *Department of Defense Dictionary of Military Terms and Associated Terms*, 12 April 2001, as amended through 30 November 2004.

[2] U.S. Army Field Manual FM 7-100, Opposing Force Doctrinal Framework and Strategy, May 2003, iv to xvi.

- Understand the nature of the terrorist threat through a concise historical review of terrorism, and basic descriptions of methods and organizational structures commonly used by terrorists and terrorist organizations.

- Understand terrorist goals and objectives, and the patterns, trends, and new techniques of terrorist operations. Acknowledging that asymmetric operations provide a significant advantage to the terrorist, the study of situational patterns and techniques in terrorism over time can offer insight and possible trends for future attacks.

- Appreciate the terrorism threat to U.S. military forces, equipment, and infrastructure.

- Relate appropriate levels of force protection (FP), operational security (OPSEC), and terrorism countermeasures based upon unit status and situation.

- Provide relevant terrorism information that applies to Active Component (AC) forces, Reserve Component (RC) Federal Reserves, and State National Guard forces in primary scenarios of being: (1) deployed on an operational mission, (2) in transit to or from an operational mission, or (3) nondeployable as a military force designated as installation or institutional support assignments.

- Complement research, analysis, and contingency techniques within a "red teaming" concept and process.[3]

Scope of the Issue

Terrorism is a significant challenge for U.S. military forces in the twenty-first century. Terrorist violence has emerged in recent years from an agenda-forcing and attention-getting tool of the politically disenfranchised to a significant asymmetric form of conflict employed against adversaries of greater economic, military, and political strength. While terrorist acts may have appeared to be extraordinary events several decades ago, today terrorism eclipses these former acts and demonstrates a profound impact on populations at the local, regional, national, and international levels. Terrorists do not plan on defeating the U.S. in a direct military confrontation. As part of a larger listing of threats, "…foes today are not trying to defeat us [U.S.] purely militarily. They're approaching this from a far broader strategic context, and in fact, they're least interested in taking us [U.S.] on head-on. They're interested in tying us down militarily, but they are really working on defeating us informationally, economically, and politically, the other dimensions of National power."[4]

---

[3] Department of Defense, Defense Science Board, *Defense Science Board Task Force on The Role and Status of DOD Red Teaming Activities*, (Washington, D.C.: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, September 2003).

[4] General Peter Schoomaker, Army Chief of Staff, "CSA Interview: Joint and Expeditionary Capabilities," (Washington, D.C.: Pentagon, 4 October, 2004), available from http://www.army.mil/leaders/leaders/csa/interviews/04Oct04.html; Internet; Accessed 11 January 2005.

Terrorism is defined by DOD as: "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."[5] This is not a universally accepted definition outside of the Department of Defense, and the study of terrorism has often been mired in a conflict over definitions and semantics. For the purposes of this handbook, this DOD doctrinal definition will be used unless otherwise noted in the text.

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.

Joint Pub 1-02

Terrorism is a special type of violence; while it has a political element, it is a criminal offense under nearly every national or international legal code. Although terrorism has not yet caused the physical devastation and large number of casualties normally associated with traditional warfare, it often produces a significant adverse psychological impact and presents a greater threat than a simple compiling of the numbers killed or the quantity of materiel destroyed would indicate.[6] An example of this is the impact on the United States of the 9/11 attacks, and the U.S. anthrax incidents. For many people around the U.S., these attacks weakened their sense of safety and security. This experience of catastrophic terrorism was evidence that the United States was not immune to attacks by international or transnational terrorist groups. Ultimately, these attacks also had severe economic impacts on the country. As Brian Jenkins testified to the 9/11 Commission, "The September 11 attack produced cascading economic effects that directly and indirectly have cost the United States hundreds of billions of dollars."[7] For other citizens, though, these terrorist acts fortified their will and resolve. Consequently, a national resolve emerged from these catastrophic incidents to combat terrorism and reassert confidence in the economy.

Terrorism is an expanding international concern too. Multinational groups in 2005 such as the Club of Madrid, comprised of former presidents and prime ministers of democratic countries, seek an international cooperation against terrorism. Principles include acknowledging terrorism as a crime against all humanity, recognizing terrorism as an attack on democracy and human rights, and rejecting any ideology that guides the actions of terrorists.[8] Similarly in March 2005, the Secretary-General of the United Nations

[5] FM 100-20, *Military Operations in Low Intensity Conflict*, 5 December 1990; and Joint Pub 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001, as amended through 9 June 2004.
[6] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 33-34.
[7] National Commission on Terrorist Attacks Upon the United States, Statement of Brian Jenkins to the Commission, March 31, 2003; available from http://www.9-11commission.gov/hearings/hearing1/witness_jenkins.htm; Internet; accessed 23 September 2004.
[8] *The Madrid Agenda*, Club de Madrid, available from http://www.clubmadrid.org/cmadrid; Internet; accessed 26 April 2005.

called for a world treaty on terrorism that would outlaw attacks targeting civilians and establish a framework for a collective response to the global threat. This might include a universal definition of terrorism, knowing that many different definitions exist currently for "terrorism," to assist in countering terrorism in all of its forms.[9]

Successful in attracting attention and creating fear and anxiety, terrorist acts often fail to translate into concrete long-term gains or achieve an ultimate objective.[10] Escalating acts of terrorism can be self-defeating when the acts become so extreme that public reaction loses attention on the terrorist's intended purpose and focuses on the acts rather than the political issue. The example of Palestinian defiance to Israeli controls in this geographic region of the Mideast illustrates how progressively more violent acts of resistance or terrorism can sometimes alienate large sections of public opinion that once may have supported a Palestinian search for recognition.[11] Thus, as a tactic, terror can be successful in its immediate purpose, but fail to achieve its ultimate aim unless dedicated political or military efforts coincide to produce tangible results. [12] When the threat or use of terrorism is used in coordination with elements such as political or military power, strategic impact may be successful. Some may see the struggle for Algerian independence or Israeli independence as strategic outcomes that used terrorism as a major instrument of influence. Others may see the 2004 Spanish withdrawal from coalition forces in Iraq as an operational outcome of terrorism in Spain, and a means toward strategic terrorist aims of fracturing the coalition and eventually causing removal of U.S. presence and prestige in the Mideast.

U.S. Strategic Overview

Defending the Nation against its enemies is the first and fundamental commitment of the Federal Government. The National Military Strategy (2004) describes ways and means for Department of Defense to protect the U.S. and win the "War on Terrorism." U.S. Joint Forces assist the Nation in preventing conflict or surprise attack, while concurrently transforming military capabilities while at war and preparing to meet future global challenges. In this contemporary operational environment, two primary U.S. concerns are terrorists of global reach and the emergent threat of terrorist use of weapons of mass destruction. The National Security Strategy (NSS) of the USA states national priorities for dealing with terrorism.

When the President of the United States of America addresses terrorism as an enemy, the enemy is not a single political regime or person or religion or ideology. "The enemy is terrorism – premeditated, politically motivated violence perpetrated against

[9] Ed McCullough, "Annan calls for treaty outlawing terrorism," Associated Press, 10 March 2005; available from http://www.kentucky.com/mld/kentucky/news/weird_news/11099663.htm?template; Internet; accessed 26 April 2005.
[10] Caleb Carr, *The Lessons of Terror: A History of Warfare Against Civilians: Why it has Always Failed and Why it will Fail Again* (New York: Random House, 2002), 11.
[11] Caleb Carr, "TIME.com Interview with Calib Carr," 1 February 2002; available at http://www.time.com/time/2002/carr/interview.html; Internet; accessed 31 August 2004.
[12] Walter Lacquer, *The New Terrorism: Fanaticism and the Arms of Mass Destruction* (New York: Oxford University Press, 1999), 48.

innocents…[U.S.] priority will be first to disrupt and destroy terrorist organizations of global reach and attack their leadership; command, control, and communications; material support; and finances."[13] The strategic intent of the U.S. National Strategy for Combating Terrorism adds a national priority of denying sanctuary to terrorist organizations with global reach.[14]

Other principal threats are rogue states or terrorist organizations – enemies − who have declared the intention to obtain and use weapons of mass destruction [WMD] against the United States of America. The September 2001 attacks on the United States demonstrated that inflicting mass casualties is one of several specific means that will be used by terrorists to spotlight an agenda. Mass casualties would be exponentially more severe if terrorists acquired and used weapons of mass destruction.[15] As noted in the U.S. National Security Strategy, the targets of these WMD attacks include U.S. military forces and civilian population.

The major institutions of American national security were designed in a different era to meet different national and global requirements. All of these security measures are transforming. This includes building and maintaining national defenses beyond challenge…an essential role exists for American military strength in near-term readiness and the ability to fight the war on terrorism.[16]

U.S. Goals and Objectives

The United States demonstrates a national resolve to ensure the protection of the Nation and reduce its vulnerability to terrorism. Although an enduring vulnerability exists, the leaders at each level of government are implementing interconnected strategies to address emerging risks and threats of terrorism. While protection infers prevention from terrorist attacks, U.S. national strategies recognize that accepting some level of terrorism risk is a permanent condition. The National Strategy for Homeland Security presents six critical mission areas for security risk management and resourcing: intelligence and warning, border and transportation security, domestic counterterrorism, protecting critical infrastructure, defending against catastrophic terrorism, and emergency preparedness and response.[17] A survey of these mission sets aligns readily with functions of expert support that U.S. military forces can provide, as an operating element of the Department of Defense, within Federal law.

---

[13] President, National Strategy, *National Security Strategy of the United States of America,* Washington, D.C. (December 2002): Introduction and Section III; available from http://www.whitehouse.gov/nsc/print/nssall.html; Internet; accessed 8 December 2003.

[14] President, National Strategy, *National Strategy for Combating Terrorism,* Washington, D.C. (February 2003): 11; available from http://www.state.gov/s/ct/rls/rm/2003/17798.htm; Internet; accessed 8 December 2003.

[15] President, National Strategy, *National Security Strategy of the United States of America,* Washington, D.C. (December 2002): Section V; available from http://www.whitehouse.gov/nsc/print/nssall.html; Internet; accessed 8 December 2003.

[16] Ibid., Section IX.

[17] President, National Strategy, *National Strategy for Homeland Security,* Washington, D.C. (16 July 2002): viii and 2; available from http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf; Internet; accessed 8 December 2003.

Of note, the United States has implemented an integrated series of national strategies to enhance the security of the Nation. These strategies translate instruments of national power into strategic, operational and tactical actions against terrorism. U.S. military forces are part of a national arsenal of capabilities among diplomatic, economic, law enforcement, financial, information, and intelligence institutions in the Global War on Terrorism (GWOT).

> **"No group or nation should mistake America's intention: We will not rest until terrorist groups of global reach have been found, have been stopped, and have been defeated."**
>
> George W. Bush
> The President of the United States of America
> September 14, 2001

Soon after the catastrophe of the 2001 World Trade Center bombing, the President of the United States declared a specific charter to U.S. military forces: "The battle is now joined on many fronts. We will not waver, we will not tire, we will not falter and we will not fail. Peace and freedom will prevail…To all the men and women in our military, every sailor, every soldier, every airman, every coast guardsman, every marine, I say this: Your mission is defined. The objectives are clear. Your goal is just. You have my full confidence, and you will have every tool you need to carry out your duty."[18] As one of several instruments of national power, the "just" goal reaches beyond a task of just preserving U.S. freedoms. This goal envisions a world with the ability for all people to live and prosper without fear.

GWOT and the Contemporary Operational Environment

On a global scale, the United States National Defense Strategy has four strategic objectives: (1) secure the United States from direct attack, (2) secure strategic access and retain global freedom of action, (3) strengthen alliances and partnerships, and (4) establish favorable security conditions. Four ways that the U.S. accomplishes those objectives are assuring allies and friends, dissuading potential adversaries, deterring aggression and coercion, and when necessary, defeating adversaries.[19] These principles are integral to situational awareness in the Global War on Terrorism (GWOT).

The GWOT is an operational environment of today and for the foreseeable future. The *Operational Environment* (OE) as defined by the Department of Defense is: "A composite of the conditions, circumstances, and influences that affect employment of

[18] "Transcript of President George Bush's address 10/07/01," ATTACK on AMERICA [database on-line]; available from http://multimedia.belointeractive.com/attack/bush/1007bushtranscript.html; Internet; accessed 13 July 2004.
[19] Department of Defense, *The National Defense Strategy of the United States of America*, (Washington, D.C.: GPO, 1 March 2005), iv.

military forces and bear on the decisions of the unit commander."[20] The U.S. Army builds on this DOD definition and further defines a mission setting for the current or near-term future circumstances – a Contemporary Operational Environment.[21]

The *Contemporary Operational Environment* (COE) encompasses a full range of terrorism threat. Originated to address known and potential *conditions, circumstances, and influences,* and adversaries that U.S. forces might confront in a post-Cold War world, the COE is a conceptual construct to recognize several norms and critical variables for military decisionmaking, planning, and operating. As a superpower, the U.S. must still consider the normal influences of diverse movements and regional powers around the world and the capabilities of their armed forces, paramilitary forces, or clandestine groups.

The U.S. National Defense Strategy identifies four types of challenging threats. Traditional challenges exist by states that employ recognized military capabilities and forces in the more conventional forms of military competition and conflict. Irregular challenges are the more unconventional ways and means to counter the traditional advantages of stronger opponents. Catastrophic challenges involve the acquisition, possession, and possible use of WMD or methods that produce WMD-like effects (WMD/E). Disruptive challenges may be the use of breakthrough technologies to limit or negate the operational advantage of an opponent.[22]

Challenging Threats

- **Traditional**
- **Irregular**
- **Catastrophic**
- **Disruptive**

The National Military Strategic Plan for the War on Terrorism (NMSP-WOT) addresses the GWOT nature of the threat, and states priorities and responsibilities within the U.S. Armed Forces. As noted by the U.S. Chairman of the Joint Chiefs of Staff, this strategy "…produces a clearer understanding of the enemies we face and the conditions under which we fight…" The nature of this environment is a war against extremists that advocate the use of violence to gain control over others, and in doing so, threaten our [U.S.] way of life. Success will rely heavily on close cooperation and integration of all instruments of national power and the combined efforts of the international community. The overall goal of this war is to preserve and promote the way of life of free and open societies based on rule of law, defeat terrorist extremism as a threat to that way of life, and create a global environment inhospitable to terrorist extremists.[23]

The Strategy for Homeland Defense and Civil Support integrates the objectives and guidance expressed in the National Security Strategy, national Strategy for Homeland Security and national Defense Strategy to guide DOD operations to protect the US Homeland. The strategy describes DOD responsibilities in terms of leading, supporting, or enabling activities and establishes the following prioritized objectives:

---

[20] Department of Defense, *DOD Dictionary of Military Terms*, available from http://www.dtic.mil/doctrine/jel/doddict/data/o/03843.html; Internet; accessed 25 April 2005.
[21] Army Field Manual 7-100, *Opposing Force Doctrinal Framework and Strategy*, (Washington, D.C.: GPO, May 2003), Foreword and iv.
[22] *The National Defense Strategy of the United States of America*, 1 March 2005, 2.
[23] Joint Chiefs of Staff, J5 War on Terrorism, Strategic Planning Division, Briefing (U) *The National Military Strategic Plan for the War on Terrorism (NMSP-WOT)*, Version 18 April 2005.

- Achieve Maximum Awareness of Threats
- Deter, Interdict, and Defeat Threats at a Safe Distance
- Achieve Mission Assurance
- Support Consequence Management for CBRNE Mass casualty Attacks
- Improve National and International Capabilities for Homeland Defense

The *Contemporary Operational Environment* (COE) has several common threads or constants for defining the environment. The U.S. will not experience a peer competitor until 2020 or beyond. Armed forces will continue to be used as a tool to pursue national interests. The U.S. may direct military action within the context of an alliance, a coalition, or even as unilateral action, with or without United Nations sanctions. Actions will be waged in a larger environment of diplomatic, informational, economic, and military operations. Modernization of capabilities by potential or known adversaries could negate U.S. overmatch for select periods of time or specific capabilities. Similarly, advanced technologies will be readily available on a world market for nation-states and non-state actors. Non-state actors can cause significant impacts on a military operation, as combatants and non-combatants. Of course, these factors and their effects will vary depending on a particular situation; however, a constant that must also be addressed is the issue of variables.

Complementing these overarching constants or factors, the U.S. Army describes eleven critical variables that enhance a comprehensive appreciation of a particular mission setting. This assessment and analysis is appropriate for both real world contingencies and training preparations. Whether a real world threat or an opposing force created to simulate realistic and relevant conditions for training readiness, the COE is a dynamic and adaptive process of being more aware, better prepared, and fully ready to counter any adversary that could negatively impact on conduct of an assigned U.S. military mission.

Critical Variables of the COE

- **Nature and Stability of the State**
- **Regional and Global Relationships**
- **Economics**
- **Sociological Demographics**
- **Information**
- **Physical Environment**
- **Technology**
- **External Environment**
- **National Will**
- **Time**
- **Military Capabilities**

(*Source:* U.S. Army Field Manual 7-100)

Interaction among these elements may range from peaceful humanitarian assistance to high-intensity combat operations. Alliances and coalitions are the expectation in most operations, but U.S. unilateral action is always a consideration. Military operations interrelate with other elements of national power – diplomatic, economic, social-cultural, and informational – for both the U.S. and an adversary. Advanced technologies are available to almost anyone, yet sophistication of weapon systems, in itself, may be a liability. Intelligence and operational tools

must overlap and integrate complex sensor-surveillance systems and the clarity of human intelligence "eyes on the ground" collection and analysis. Engagement among significant actors in the COE can span formal nation-state representatives to the impact of individual combatants and noncombatants. Acts of terrorism are part of this reality.

The United States will target eight major terrorist vulnerabilities. This targeting is against terrorist networks, including state and non-state supporters. The complexity of the contemporary operational environment can be assessed as "…the most dangerous times of our lifetime…not so much because we know precisely what somebody's going to do, when and where, or how they're going to do it; but that we know their intent and we know what the possibilities are and we know what our vulnerabilities are…So terrorism is part of the tactic. In other ways it's [terrorism] an 'ism', much like communism and the others, only so much as it's embodied in whatever movements and for whatever reasons."[24] The intent is to maintain the initiative and dictate the tempo, timing, and direction of operations against terrorism. Disrupting terrorist capabilities include the channels for accepting recruits to fill terrorists ranks; the terrorist ability to plan, train, and operate; the terrorist access to critical information and intelligence, and the terrorist ability to travel, conduct reconnaissance and surveillance, or command and control.

Terrorist Vulnerabilities

- **Ideological Support**
- **Leadership**
- **"Foot Soldiers"**
- **Safe Havens**
- **Weapons**
- **Funds**
- **Communications and Movement**
- **Access to Targets**

Source: National Defense Strategy, March 2005

Assessing the Threat

- **Mapping the Threat**
- **Analyzing Networks**
- **Planning Actions**
- **Determining Metrics**
- **Tracking Actions**
- **Evaluating Outcomes**
- **Adapting Methods**
- **Improving Results**

As an example, denying resources to terrorists and terrorist networks is critical to countering the ideological support of terrorism. These efforts remove any legitimacy to terrorism and eliminate state and private support for terrorism; make it politically unsustainable for any country to support or condone terrorism; and support models for moderation in the Muslim regions of the world. Techniques in coordinating such actions may include a methodology of identifying or "mapping" key components that affect resources such as technology, key figures, and locations. Identifying the major connections among these components can spotlight weak assailable links of the networking and

[24] General Peter Schoomaker, U.S. Army Chief of Staff, "Media Roundtable at the Association of the United States Army Annual Convention, Washington, D.C., 4 October 2004; available from: http://www.army.mil/leaders/leaders/csa/interviews/04Oct04Roundtable.html; Internet; accessed 11 January 2005.

where targeting and action plans may be most effective. Measuring results and adapting operations enable a process for improved Joint leader education, training, and GWOT operations.[25]

Red Teaming

Key to combating terrorism is the process of Red Teaming. As a time-proven concept used in U.S. government and commercial enterprises, red teaming deepens the understanding of options that are available to counter adaptive adversaries. This methodology both complements and informs intelligence collection and analysis, and enhances predictive estimates of adversary capabilities and intentions. Aggressive red teams challenge emerging operational concepts, evolving contingency plans, as well as operational orders in order to discover weaknesses before real adversaries do. The perspective of an adversary may be that of a confirmed threat, or a contingency of threat capabilities used to present conditions, circumstances, and influences for training and readiness.

Threat and Opposing Force

Threat - Any specific foreign nation or organization with intentions and military capabilities that suggest it could become an adversary or challenge the national security interests of the United States or its allies.

U.S. Army Regulation 350-2

Opposing Force (OPFOR) – A plausible, flexible military and/or paramilitary force representing a composite of varying capabilities of actual worldwide forces, used in lieu of a specific threat force, for training and developing U.S. forces.

U.S. Army Regulation 350-2

In 2003, a Defense Science Board task force validated two primary reasons for expanding the role of red teaming in the DOD: (1) To deepen understanding of the adversaries the U.S. now faces in the war on terrorism and in particular their capabilities and potential responses to U.S. initiatives, and (2) To guard against complacency. Red teaming can stress concepts, plans, and systems to identify vulnerabilities and capabilities before direct confrontation with a real world adversary. To best apply red teaming programs, red team members must be able to understand the thinking and motivations of adversaries with different cultural and social backgrounds, to assess and analyze acting as independent and adaptive adversaries, and to interact and recommend in constructive and creative ways with the supported friendly forces leader and military decisionmaker.[26]

The overarching aim of this handbook is to create situational awareness and understanding of current terrorism capabilities and limitations, and complement the

[25] Joint Chiefs of Staff, J5 War on Terrorism, Strategic Planning Division, Briefing (U) *Countering Ideological Support for Terrorism*, Version 19Jan05, 5 April 2005.
[26] Department of Defense, Defense Science Board, *Defense Science Board Task Force on The Role and Status of DOD Red Teaming Activities*, (Washington, D.C.: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, September 2003), 1, 15, 16, and Appendix 1.

deliberate processes of military risk management, force protection, and mission orders conduct and leader decision-making. U.S. Armed Forces are at war – a Global War on Terrorism. In this long-term war of uncertain duration, the United States of America will continue to defend its values, liberties, and culture; its economic prosperity; and its security. U.S. Armed Forces are essential to this defense.

This Page Intentionally Blank

Section I: General –WMD/E Consequence Management

The targets for terrorist WMD attacks are U.S. military forces and the civilian population.

U.S. National Security Strategy

"Defending the [U.S.] Nation against its enemies is the first and fundamental commitment of the U.S. Federal Government…The gravest danger our Nation faces lies at the crossroads of radicalism and technology. Our enemies have openly declared that they are seeking weapons of mass destruction, and evidence indicates that they are doing so with determination…we must be prepared to defeat our enemies' plans, using the best intelligence and proceeding with determination."[27]

The U.S. National Security Strategy states a compelling requirement to stop rogue states and their terrorist clients before they are able to threaten or use weapons of mass destruction against the United States and our allies and friends.[28] National Security Presidential Directive 17, the *National Strategy to Combat Weapons of Mass Destruction*, calls for a comprehensive action plan to counter the threat of WMD in all of its dimensions. This strategy component is integral to the Global War on Terrorism (GWOT), U.S. homeland security, and other national strategies to defend and protect the United States. Three main pillars describe the essential aspects of combating weapons of mass destruction: counter proliferation, improved nonproliferation, and when necessary, effective consequence management to a WMD incident.

Figure. I-1. **Nuclear Plant Photo**
(*Source*: National Strategy for Homeland Security [minus reticle])

[27] The White House, *The National Security Strategy of the United Sates of America*, 1, 17 September 2002; available at http://www.whitehouse.gov/nsc/nss.html; Internet; accessed 30 April 2004.
[28] *National Security Strategy*, 9.

As a primary objective, terrorists attempt to create a demoralizing psychological effect on the target population and its leaders to erode resolve and enhance terrorist objectives. The characteristics of the United States – freedom, systems of movement, modern life, and prosperity – are all vulnerable to terrorism. Meanwhile, the distinction between domestic and foreign affairs is diminishing. The U.S. military and other appropriate agencies at Federal, state, and local levels of government must be prepared to deter and defend against the full range of possible WMD attack. Homeland security and transforming defense capabilities are part of this readiness. Of particular note, the U.S. must maintain the capability to reduce to the extent possible, the potentially horrific consequences of WMD attacks in the U.S. Homeland and at locations around the world.[29]

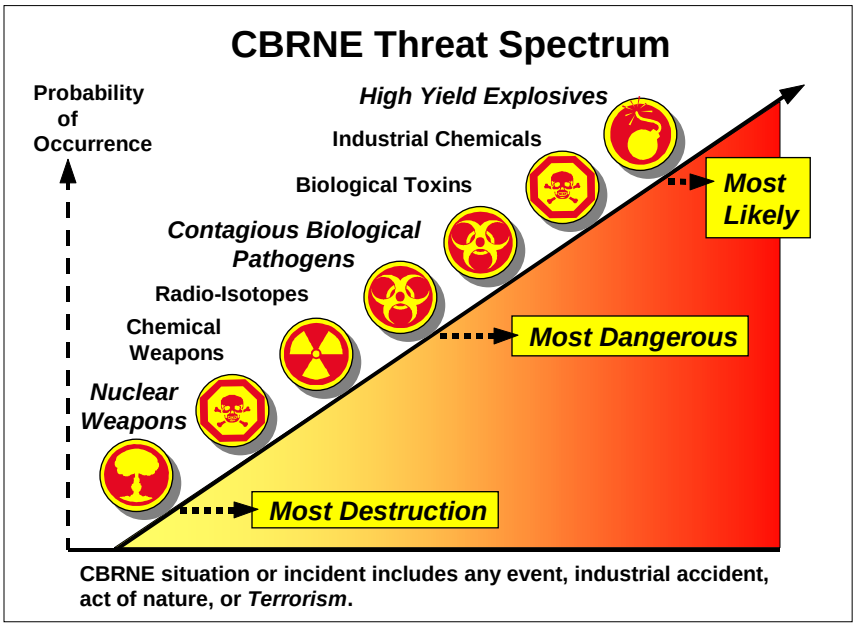

Figure I-2. **CBRNE Threat Spectrum**
(*Source*: JTF Civil Support Command Briefing 2005 and JHM).

To appreciate U.S. military capabilities for consequence management of a CBRNE incident, situational awareness must understand the probability of terrorist attack with chemical, biological, radiological, nuclear, or high yield explosive explosives. U.S. military capabilities are integral to a larger, robust national ability to prevent such attacks, mitigate their impact if they do occur, and respond with DSCA in a coordinated effort to assist the affected population. The Department of Defense (DOD) supports this Federal mandate – the National Response Plan (NRP) – with centralized command and control and robust capabilities of DOD forces to assist a lead agency in a domestic CBRNE[30]

[29] The White House, National Security Presidential Directive 17 (NSPD-17), *National Strategy to Combat Weapons of Mass Destruction*, 2, December 2002; available at http://www.fas.org/irp/offdocs/nspd/nspd-17.html; Internet; accessed 8 December 2003.
[30] CJCSI 3125.01 *Military Assistance to Domestic Consequence Management Operations in Response to a Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive Situation*, 3 August 2001.

incident caused by a WMD weapon, device, or material specifically designed to produce mass casualties or terror. One superb example of DOD consequence management capability is USNORTHCOM Joint Task Force Civil Support. However, to better appreciate the compelling requirements and capabilities of JTF Civil Support, the specter of WMD and terrorism must be fully understood.

Response actions are immediate and short-term activities to preserve life, property, the environments, and the social, economic, and political structure of the affected community. In the context of a terrorist threat, simultaneous activities assess regional and national-level impacts, as well as access and take appropriate action to prevent and protect against other potential threats.[31]

[31] U.S. Department of Homeland Security, *National Response Plan*. Washington, D.C.: U.S. Department of Homeland Security, November 2004, 53.

Page Intentionally Blank

Section II: Global Reach and WMD Terrorism

The probability of a terrorist organization using a chemical, biological, radiological, or nuclear weapon, or high yield explosive has increased significantly during the past decade.[32] The April 2004 terrorist attempt to simultaneously bomb locations in Jordan with high yield explosives and chemical weapons spotlights the deliberate planning for use of weapons of mass destruction. Fortunately, Jordanian authorities foiled this attack on Jordanian and U.S. targets with a preemptive raid on terrorist facilities. Reports estimate that 20 tons of chemicals were confiscated and could have caused tens of thousands of casualties.[33] The intent of U.S. strategy is to stop terrorist attacks against the United States, its citizens, its interests, and its friends and allies around the world, and ultimately, to create an international environment inhospitable to terrorists and all those who support them.[34] The U.S. will not ignore regional or emerging threats, however, the operational efforts and intelligence will focus primarily on the most dangerous groups, namely, those terrorist groups with global reach or aspirations to acquire and use WMD.[35]

The 2004 U.S. National Military Strategy introduces an emergent term of weapons of mass destruction or effect (WMD/E). The term WMD/E relates to a broad range of adversary capabilities that pose potentially devastating impacts. WMD/E includes chemical, biological, radiological, nuclear, and enhanced high explosive weapons as well as other, more asymmetrical "weapons." They may rely more on disruptive impact than destructive kinetic effects. For example, cyber attacks on U.S. commercial information systems or attacks against transportation networks may have a greater economic or psychological effect than a relatively small release of a lethal agent.[36]

To enhance national security measures against terrorism and use of WMD, the U.S. uses several complementing strategies. Two of these strategies are the *National Strategy for Homeland Security* and the *National Strategy for Combating Terrorism*. Another directive is the *National Strategy to Combat Weapons of Mass Destruction*. While the strategy for homeland security focuses on preventing terrorist attacks within the United States, the strategy for combating terrorism focuses on identifying and defusing threats before they reach our borders.[37] Nonetheless, concepts of homeland security and combating terrorism, especially WMD and terrorism, are inseparable. U.S. strategic objectives seek to protect the U.S. from terrorism, reduce U.S. vulnerabilities, minimize damage, and recover from attacks that do occur.[38] In assessing functional capabilities, critical U.S. mission areas include: intelligence and warning, border and transportation

---

[32] The White House, *National Strategy for Combating Terrorism*, 9, February 2003; available at http://www.state.gov/s/ct/rls/rm/2003/17798.htm; Internet; accessed 30 April 2004.
[33] "Jordan 'was chemical bomb target'," BBC News UK Edition, 17 April 2004; available at http://news.bbc.co.uk/1/hi/world/middle_east/3635381.stm; Internet; accessed 28 April 2004.
[34] *National Strategy for Combating Terrorism*, 11.
[35] Ibid., 16.
[36] Joint Chiefs of Staff, *National Military Strategy of the United States of America*, 1, May 2004.
[37] *National Strategy for Combating Terrorism*, 2.
[38] *National Strategy for Homeland Security*, vii.

security, domestic counterterrorism, protecting critical infrastructure, defending against catastrophic terrorism, and emergency preparedness and response.[39]

Incidents of National Significance

Incidents that require Department of Homeland Security (DHS) operational and resource coordination are termed *Incidents of National Significance,* also referred to as nationally significant incidents or national incidents. Incidents requiring DHS action can include events such as: (1) credible threats, indications of terrorism or acts of terrorism within the United States; (2) major disasters or emergencies as defined under the Robert T. Stafford Disaster Relief and Emergency Assistance Act,[40] or any instances when the U.S. President determines that Federal assistance is needed to supplement state and local efforts to save lives and to protect property and public health and safety; (3) catastrophic natural or manmade incidents, including terrorism, that results in extraordinary levels of mass casualties, damage, and disruption severely affecting the population, infrastructure, environment, economy, national morale, and government functions;[41] or (4) unique situations that may require coordination of incident management efforts.

Such incidents could include credible threats, indications or warnings of imminent terrorist attack, or acts of terrorism directed domestically against the people, property, environment, or political or legal institutions of the United States or its territories or possessions; and threats or incidents related to high profile, large-scale events that present high-probability targets such as National Special Security Events (NSSE) and other special events as determined by the Secretary of Homeland Security, in coordination with other Federal departments and agencies.[42]

Immediate response is a concept that applies to unique circumstances and allows commanders to respond immediately, prior to a Federal declaration, to imminently serious conditions that are beyond the capability of local authorities. Local commanders can respond immediately to request for assistance to save lives, to prevent human suffering, and to mitigate great property damage. Immediate information must be provided to the DOD Executive Agent through the military chain of command. This type of response is normally of very short duration and will not normally exceed 72 hours of operations.

Crisis and the National Response Plan (NRP)

Response to national crises or consequence management to a catastrophic incident has evolved into a fully integrated national emergency response system. The Department of

[39] Ibid., viii.
[40] The *Robert. T. Stafford Disaster Relief and Emergency Assistance Act,* 42 U.S.C. 5121-5206, establishes the programs and processes for the Federal government to provide disaster and emergency assistance to States, local governments, tribal nations, individuals and qualified private non-profit organizations. The provisions of the Stafford Act cover all hazards including natural disasters and terrorist events. See glossary for an expanded description of significant provisions for DOD defense support to civilian authorities.
[41] *National Response Plan,* Nov 2004, 43.
[42] Ibid., 4.

Homeland Security (DHS) consolidated multiple Federal response plans into a unified, all-discipline, and all-hazards approach to domestic incident management. The Federal Response Plan was published in November 2004. The NRP serves as the core strategic national-level plan for coordinating Federal incident management activities for terrorist attacks. This plan is a consistent doctrinal framework, using the National Incident Management System (NIMS), for incident management at all jurisdictional levels.[43]

WMD Incident Management Phases[44]

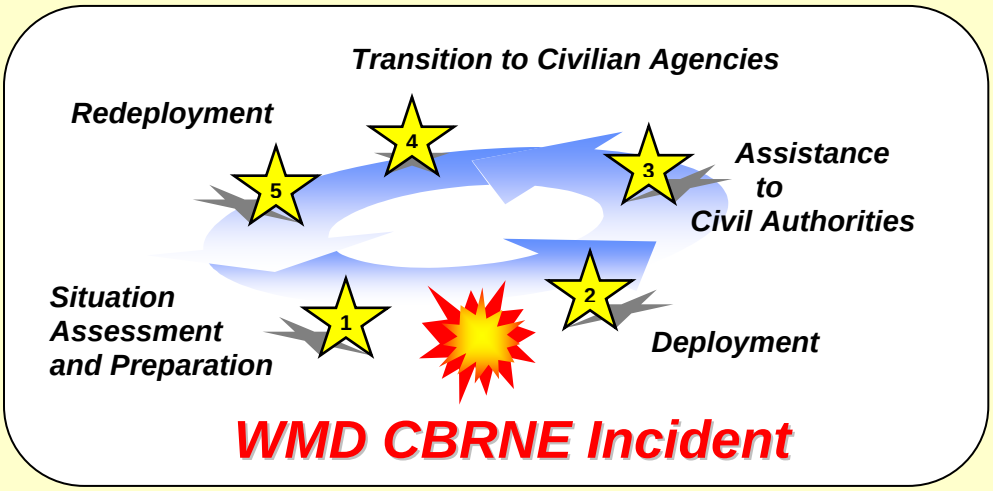

Figure. II-1. **WMD CBRNE Incident Management Phases**
(*Source*: JTF Civil Support J5 2005 and JHM)

The hazard-specific incident annexes in the NRP spotlight the type of national incidents, events, and hazards that may require a unified, specialized response: catastrophic incident; oil and hazardous materials; nuclear and radiological; biological; food safety and agriculture; cyber; and terrorism incident law enforcement and investigation. [45]

The Homeland Security Act of 2002 represents a crucial transition point in the way the Federal government organizes emergency response to WMD terrorism. The Act establishes the Department of Homeland Security (DHS), and consolidates the consequence management missions, assets, and personnel of numerous Federal departments and agencies into a single department. The primary missions of DHS

[43] Ibid., i.
[44] CJCS CONPLAN 0500-98, *Military Assistance to Domestic Consequence Management Operations in Response to a Chemical, Biological, Radiological, Nuclear, or High-Yield Explosive Situation*, 11 February 2002.
[45] Ibid., xii-xiii.

include: preventing terrorist attacks within the United States; reducing the vulnerability of the United States to terrorism; and minimizing the damage and assisting in the recovery from terrorist attacks that occur within the United States.[46] The Homeland Security Act consolidates WMD consequence management assets and personnel under a single Federal agency, and serves as the legal impetus for a revised approach to WMD incident management.

Civil Response Process

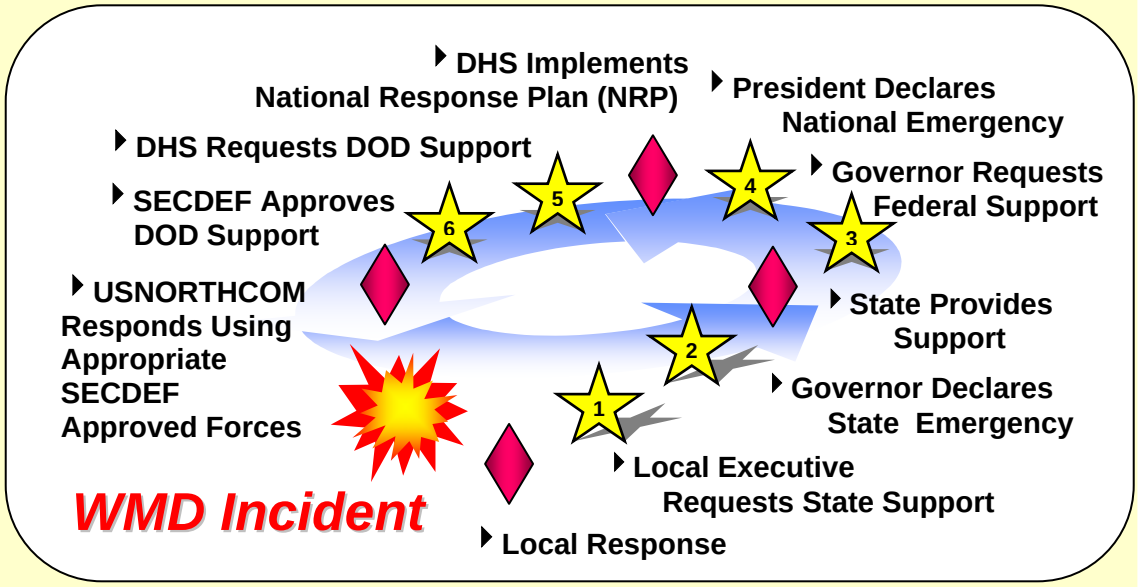

Figure. II-2. **Civil Response Process**
(*Source:* JTF Civil Support J5 2005 and JHM)

HSPD-5 and the Federal Response Structure

Homeland Security Presidential Directive 5 (HSPD-5), *Management of Domestic Incidents*, establishes a new approach to Federal emergency management of WMD events. The directive ensures that all levels of government across the nation have a single, unified, national approach toward managing domestic incidents. In conjunction with the *Homeland Security Act of 2002*, HSPD-5 tasks the Secretary of Homeland Security to develop and administer a National Response Plan that integrates Federal government domestic prevention, preparedness, response and recovery plans into one all-discipline,

[46] Defense Threat Reduction Agency, *Domestic WMD Incident Management Legal Deskbook*, 3-12 and 3-13, December 2003; available at http://biotech.law.lsu.edu/blaw/DOD/manual; Internet; accessed 23 April 2004.

all-hazards plan. It also tasks the Secretary of Homeland Security to develop and administer a National Incident Management System (NIMS) that would unify Federal, state and local government capabilities within a National Response Plan framework to prepare for, respond to and recover from domestic events regardless of cause, size or complexity. These three echelons of government capability are three mutually supporting pillars of emergency response and civil support.

The intent behind the NRP is to provide the structure and mechanisms for establishing national level policy and operational direction regarding Federal support to state and local incident managers. The NRP establishes the Federal government's response policy, whereas the NIMS serves as the operational arm of the NRP. The NIMS improves the chain of national command authority and coordination among the many Federal, state, and local organizations; improves planning and readiness; and integrates crisis and consequence management.

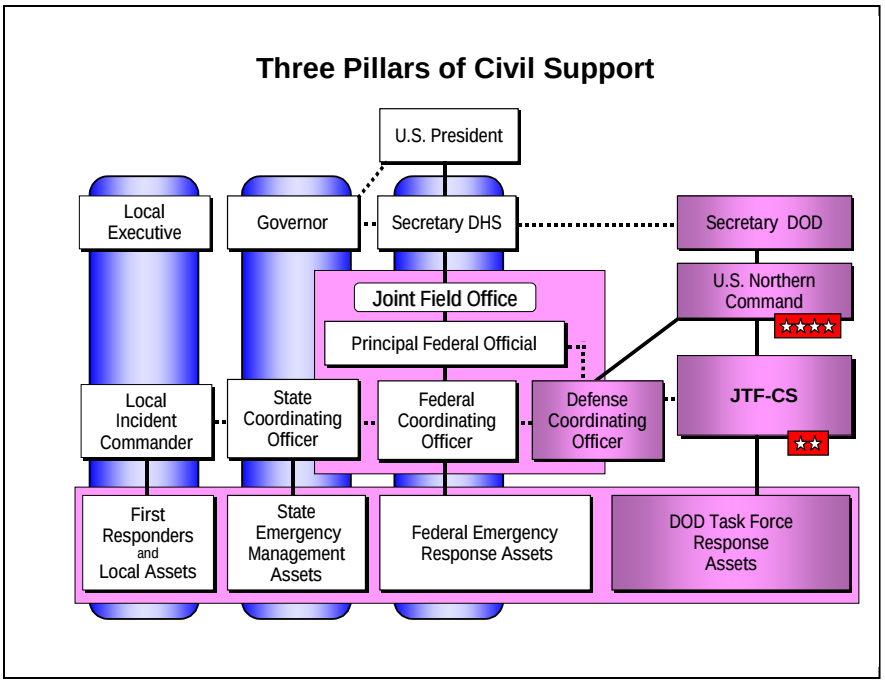

Figure. II-3. **Three Pillars of Civil Support**
(*Source*: JTF Civil Support Command Briefing 2005 and JHM)

HSPD-5 also reaffirms the Secretary of Homeland Security's responsibility as the principal Federal official for domestic incident management. This coordination responsibility exists when any one of the following four conditions applies: (1) a Federal department or agency acting under its own authority has requested the assistance of the Secretary; (2) the resources of state and local authorities are overwhelmed and Federal assistance has been requested by the appropriate state and local authorities; (3) more than one Federal department or agency has become substantially involved in responding to the

incident; or (4) the Secretary has been directed to assume responsibility for managing the domestic incident by the President.

HSPD-5 also eliminates the previous division between crisis management[47] and consequence management[48] treating the two "as a single, integrated function, rather than as two separate functions." Whereas under the Federal Response Plan the Attorney General was the overall lead Federal official for the Government's response until the crisis management phase of the response was over, now the Secretary of Homeland Security remains the lead Federal official for the duration of the period involving Federal assistance. Despite HSPD-5 erasing the distinction between crisis management and consequence management, the directive reaffirms the Attorney General's authority as the lead official for conducting criminal investigation of terrorist acts or terrorist threats.[49]

[47] *Crisis Management*. Traditionally, crisis management was predominantly a law enforcement function and included measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism. The requirements of consequence management and crisis management are combined in the NRP.
[48] *Consequence Management.* Traditionally, consequence management has been predominantly an emergency management function and included measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism. The requirements of consequence management and crisis management are combined in the NRP.
[49] DTRA *Domestic WMD Incident Management Legal Deskbook*. 3-14.

Section III: Improvements to Incident Response

Approval of the National Response Plan (NRP) provides improved incident management capability to the U.S. Several coordination processes and procedures implement a more effective emergency response. Some of the more visible capabilities are a National Homeland Security Operations Center (HSOC). The HSOC serves as the primary national-level hub for operational communications and information pertaining to domestic incident DHS headquarters, the HSOC provides full-time threat monitoring and situational awareness for domestic incident management. An Interagency Incident Management Group (IIMG), comprised of senior representatives from Federal departments and agencies, non-governmental organizations, as well as DHS components, facilitates national-level situation awareness, policy coordination, and incident coordination.

Correspondingly at an incident, Federal organization and principal leaders function, some with new titles and expanded responsibilities, for improved command and control, incident management and consequence management.

Joint Field Office (JFO). The JFO is a temporary Federal headquarters established to unify the Federal assistance effort with the state and local levels, and to coordinate the provision of Federal assistance to affected areas during national incidents. The JFO provides a central point for Federal, state, and local executives for incident oversight, direction, and assistance to effectively conduct and coordinate prevention, preparedness, response and recovery actions. The JFO leadership is responsible for coordination and integration of Federal operations and resources with state, local, private sector, and non-governmental organization incident command structures.

The JFO utilizes a scalable structure of the NIMS Incident Command System[50] and incident civilian "unified command."[51] The JFO organization adapts to the magnitude of the incident and supports NIMS principles regarding span of control and the five functions of: command, operations, planning, logistics, and finance/administration. Law enforcement activities are managed through the JOC, which becomes the operational branch of the JFO during terrorist-related Incidents of National Significance, when required.[52]

---

[50] *The Incident Command System* (ICS) is a standardized on-scene emergency management concept specifically designed to adopt an integrated organizational structure equal to the complexity and demands of single or multiple incidents without being hindered by jurisdictional boundaries. The national standard for ICS is provided by NIMS. An Incident Commander (IC) provides Federal overall authority and responsibility for conducting the incident management. See *NRP*, Nov 2004, 67. This is NOT "command" as defined by the Department of Defense.

[51] *Unified Area Command*, as a term in this Federal application of the Incident Command System (ICS), uses a definition of agencies working together through their designated Incident Commanders at a single Incident Command Post (ICP), when incidents are multi-jurisdictional, to establish a common set of objectives and strategies, allocate critical resources according to priorities, and a single Incident Action Plan. See *NRP*, Nov 2004, 63 and 73. This is NOT "unified command" as defined by the Department of Defense.

[52] *National Response Plan*, DE 2005, 28.

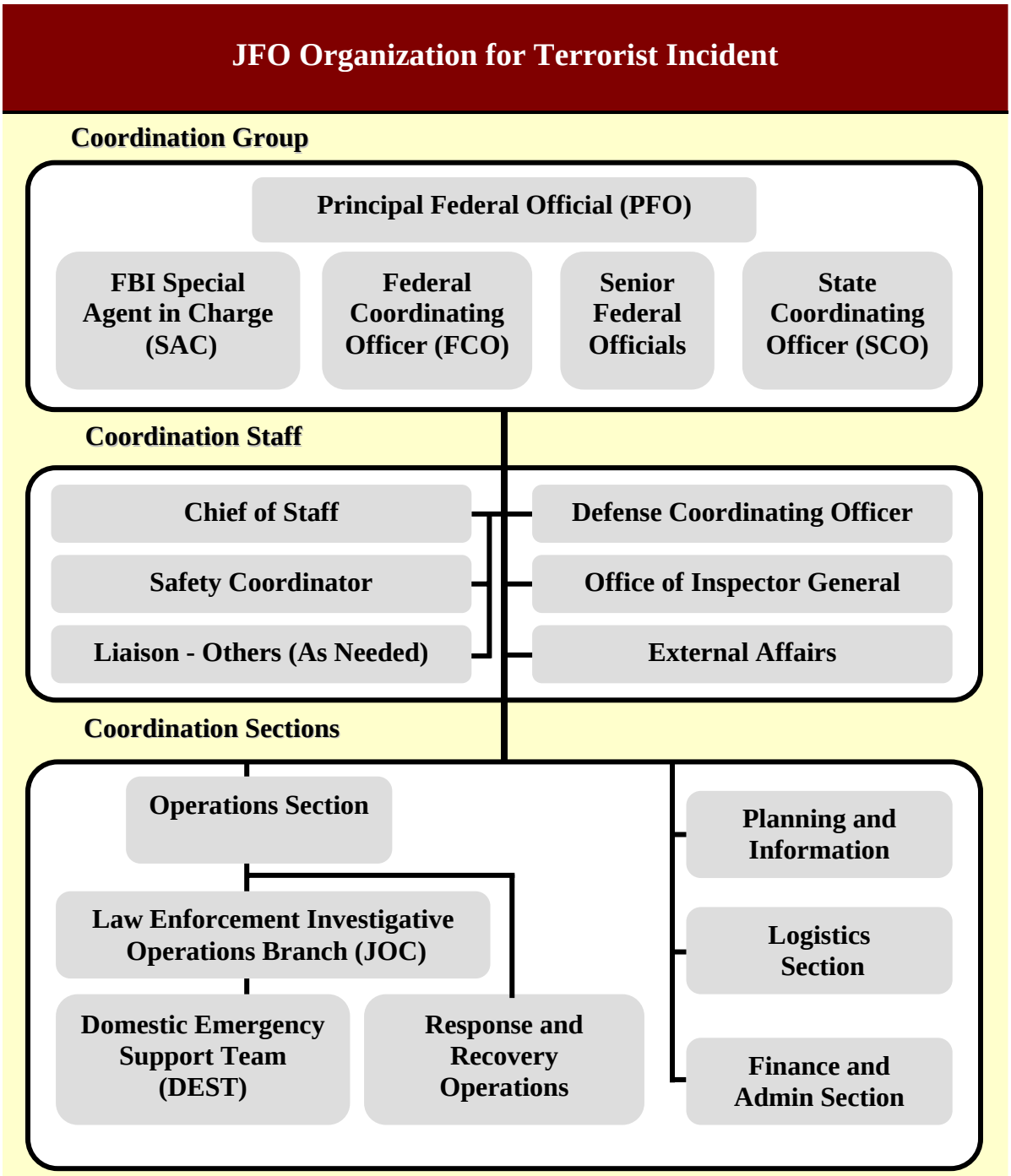

Figure III-1. **JFO Organization for Terrorist Incident**
(*Source:* National Response Plan, Dec 2005, 30.)

Personnel from state and Federal departments and agencies provide staffing for the JFO generally through their respective Emergency Support Functions (ESF). The JFO replaces the Federal Emergency Management Agency (FEMA) Disaster Field Office

(DFO) and manages all disaster assistance and other support. When activated for a terrorist incident, the JFO coordinates the functions of the Federal Bureau of Investigation (FBI) Joint Operations Center (JOC), and DHS/FEMA emergency preparedness and response and recovery actions within one Federal facility, when possible. Other Federal operations centers are encouraged to collocate with the JFO whenever possible. When the JFO is activated to support a NSSE or other security coordination function, the DHS/U.S. Secret Service (USSS) Multiagency Command Center (MACC) and the FBI JOC are collocated in the JFO when possible.[53]

Emergency Response Team (ERT). The ERT is the principal interagency group that supports the Principal Federal Officer (PFO) and Federal Coordinating Officer (FCO) in coordinating the overall Federal incident operation. The ERT provides scalable staffing and organization for the JFO. Typically, the ERT encompasses the JFO Coordination Group, JFO Coordination Staff and the four JFO areas of operations, planning and information, logistics, and finance and administration. The ERT-A, an advanced element of the ERT, is in essence the nucleus of the eventual emergency response team. Response during the early stages of an incident assesses incident impact and identifies specific state requests for Federal incident management assistance. A national headquarters-level team known as the ERT-N can be deployed for large-scale, high-impact events. [54]

Federal Incident Response Support Team (FIRST). The FIRST is a forward component of the ERT-A that provides on-scene support to the local incident command or area command structure. The FIRST deploys within two hours of notification in order to be on the scene within 12 hours of notification. This team does not supplant existing capabilities, but does provide an immediate Federal presence to the scene of an Incident of National Significance.[55]

Principal Federal Official (PFO). When an incident requires a Principal Federal Officer, the PFO is personally designated by the Secretary of Homeland Security. The purpose of a PFO is to facilitate Federal support and coordinate overall Federal incident management and assistance activities. The PFO does not replace or direct the incident command structure at the incident. The PFO does not have directive authority over the SFLEO, FCO, or other Federal or State officials. The intent of a PFO is that of coordinator and to act as a channel for media and public communications. The PFO is an interface with all appropriate jurisdictional officials involved in an incident.[56]

An "initial PFO" may facilitate near-term Federal incident management activities until a longer-term PFO designate is assigned. The Secretary of DHS provides formal notification of the appointment of a PFO to the Governor of an affected state, and uses the HSOC to notify other Federal, state, local emergency operations centers.

[53] Ibid., 28.
[54] Ibid., 40.
[55] Ibid., 41.
[56] Ibid., 33-34.

Principal Federal Official (PFO)

- **Represent Secretary of Homeland Security as lead Federal official on-scene.**
- **Ensure overall coordination of Federal domestic incident management activities and resource allocation on-scene.**
- **Ensure seamless integration of Federal incident management activities in support of State, local, and tribal requirements.**
- **Provide strategic guidance to Federal entities.**
- **Facilitate interagency conflict resolution, as necessary.**
- **Serve as primary, although not exclusive, point of contact for Federal interface with state, local, and tribal government officials, media, and private sector.**
- **Provide real-time incident information, using the Federal incident management structure on-scene, to Secretary of Homeland Security through the Homeland Security Operations Center (HSOC) and Interagency Incident Management Group (IIMG), as required.**
- **Coordinate response resource needs between multiple incidents as necessary or as directed by the Secretary of Homeland Security.**
- **Coordinate overall Federal strategy locally to ensure consistency of Federal interagency communications to the public.**
- **Ensure adequate connectivity is maintained between the JFO and HSOC; local, county, State, and regional emergency operations centers (EOC); nongovernmental EOCs; and relevant elements of the private sector.**
- **Participate in on-going steady-state preparedness efforts, as pre-designated.**

Figure III-2. **Principal Federal Official**
(*Source*: National Response Plan, Dec 2005, 33-34, and JHM)

Federal Coordinating Officer (FCO)

- **Conduct initial appraisal of the types of assistance most urgently needed.**
- **Coordinate timely delivery of Federal assistance to affected State, local, and tribal governments, and disaster victims.**
- **Support the Principal Federal Officer (PFO), when a PFO is designated.**
- **Serve as Disaster Recovery Manager (DRM) to administer the financial aspects of assistance authorized under the Stafford Act, when delegated.**
- **Work in partnership with the State Coordinating Officer (SCO) appointed by the Governor to oversee operations for the State, and the Governor's Authorized Representative (GAR) empowered by the Governor to execute all necessary documents for Federal assistance on behalf of the State.**
- **Take other such actions consistent within the delegated authority deemed necessary to assist local citizens and public officials in promptly obtaining assistance to which they are entitled.**

Figure III-3. **Federal Coordinating Officer**
(*Source*: National Response Plan, Dec 2005, 34 and JHM)

Federal Coordinating Officer (FCO). The FCO manages Federal resource support activities related to Stafford Act disasters and emergencies. The FCO supports the PFO, when one is appointed, and is responsible for directing and coordinating the timely delivery of Federal disaster assistance resources. Where a PFO is not appointed by the Secretary of Homeland Security, the appointed FCO provides overall coordination for the Federal components of the JFO and works closely with the State Coordinating Officer (SCO). The FCO works closely with the PFO, Senior Federal Law Enforcement Official (SFLEO), and other Senior Federal Officials (SFOs) representing other Federal agencies engaged in the incident management.[57]

Senior Federal Law Enforcement Official (SFLEO). The SFLEO is the senior law enforcement official from the agency with primary jurisdictional responsibility for an incident. The SFLEO directs intelligence and investigative law enforcement operations

[57] Ibid., 34-35.

related to the incident, and supports the law enforcement component of the unified command on-scene. In a terrorist event, the official will normally be the FBI Senior Agent in Charge (SAC).[58] For terrorist incidents, the President's responsibilities for coordinating and conducting law enforcement and criminal investigation activities are executed by the Attorney General acting through the FBI. During the terrorist incident, the local FBI Senior Agent in Charge (SAC) coordinates these activities with the other members of the law enforcement community, and works in conjunction with the PFO who coordinates overall Federal incident management activities.

Other Federal Teams. Examples of other specialized teams that are available to support incident management and disaster response are: Nuclear Incident Response Team (NIRT), Disaster Mortuary Operational Response Team (DMORT), or Domestic Emergency Support Team (DEST).[59] The DEST is a rapidly deployable, specialized interagency team designed to provide expert advice, guidance and support to the FBI Senior Agent in Charge (SAC) and PFO during a WMD incident or credible threat.

[58] Ibid., 35.
[59] Ibid., 41.

Section IV: Homeland Security and DOD Military Support

The Department of Defense (DOD) primarily maintains readiness to defend the USA. DOD also maintains readiness to provide Defense Support to Civil Authorities (DSCA) when directed to do so by the President of the United States (POTUS). The role of DOD in homeland security continues to gain definition. Currently, homeland security is a concerted national effort to prevent terrorist attacks within the U.S., reduce U.S. vulnerability to terrorism, minimize damage, and assist in the recovery from attacks.

The DOD role in homeland security is: (1) homeland defense as the military protection of United States territory, domestic population, and critical defense infrastructure and assets from external threats and aggression; and (2) civil support to U.S. civil authorities for domestic emergencies and for designated law enforcement and other activities.[60] The Strategy for Homeland Defense and Civil Support focuses on achieving DOD's primary strategic objective of securing the US from direct attack through an active, layered defense concept that seamlessly integrates US capabilities in the forward regions, in the approaches, and within the US Homeland. U.S. Northern Command (USNORTHCOM) was created to improve command and control of DOD forces in homeland defense and civil support missions.

For homeland defense, the DOD Services (Army, Navy, Marines, Air Force) provide USNORTHCOM, and in specific cases U.S. Pacific Command (USPACOM), with capabilities that span air, land, and sea areas as well as selected critical infrastructure. USNORTHCOM's area of responsibility comprises the air, land, and sea approaches from 500 nautical miles to the United States coastline, the continental United States itself, Alaska, Canada, Mexico, Puerto Rico, and the Virgin Islands. Hawaii and the U.S. territories and possessions in the Pacific remain the responsibility of the Pacific Command. For increased domestic airway security, USNORTHCOM coordinates the capabilities of North American Aerospace Defense Command (NORAD) and the Federal Aviation Administration. Federalized National Guard units are another capability that USNORTHCOM coordinates for homeland security efforts.[61] Numerous other DOD support capabilities exist. [62]

The National Guard has Weapons of Mass Destruction Civil Support Teams (WMD-CST) that are full-time active duty personnel whose mission is to assess a suspected CBRN[63] incident, advise civilian authorities, and expedite the arrival of additional military personnel. They can be employed in a Federal or a non-Federal status. The National Guard is normally employed in a non-Federal status, under state control, to meet the needs of state and local authorities. Each team consists of 22 personnel and is equipped with CBRN detection, analysis, and protective equipment. The U.S. Congress

[60] Department of Defense, *Report to Congress on The Role of the Department of Defense in Supporting Homeland Security*, (Washington, D.C., September 2003), 1.
[61] Steve Bowman, *Homeland Security: The Department of Defense's Role*, Congressional Research Service Report for Congress, Order Code RL 31615, 7, 14 May 2003.
[62] Ibid., 7.
[63] *CBRN*: Chemical, biological, radiological, and nuclear weapons.

has authorized 55 WMD-CSTs to ensure that each state and territory has a team. Over half of the 55 authorized teams are certified with requisite training and equipment. Remaining teams are still being staffed and equipped.[64]

The U.S. Marine Corps maintains a Chemical, Biological Incident Response Force that is capable of agent detection and identification; casualty search, rescue, and personnel decontamination; and emergency medical care and stabilization of contaminated personnel.

The U.S. Navy has been tasked to support USNORTHCOM's mission to deter and defend against hostile action from maritime threats by providing defense in depth that is seamless, unpredictable to our enemies, and able to defeat threats at a maximum distance from U.S. territory. The Navy maintains alert ships and aircraft on both coasts and the Gulf of Mexico for this mission. [65]

The U.S. Air Force has increased its "24 hours a day, 7 days a week" capabilities in a variety of ways to respond to Federal taskings under Title 10 and non-Federal taskings and Title 32 (Federally funded, state controlled) authorities. Extensive mobilization of Guardsmen and Reservists provide a robust capability posture. Aircraft Alert Posture sites have more than doubled since September 11, 2001. Combat air patrols are employed for national security special events (NSSEs) and other designated public venues, as required. The Air Force Auxiliary (Civil Air Patrol) provides additional capacity to support USNORTHCOM, other Federal agencies, and state and local governments. [66]

DOD and Defense Support of Civil Authorities

Defense Support of Civilian Authorities

DSCA refers to Department of Defense support provided by Federal military forces, DOD Civilians and contract personnel, and DOD agencies and components, in response to requests for assistance during domestic incidents to include terrorist threats or attacks, major disasters, and other emergencies.

National Response Plan
December 2005

The Department of Defense provides Defense Support of Civil Authorities (DSCA) in response to requests for Federal assistance during domestic terrorist attacks, major disasters, and other emergencies. Although current DOD Directives use terms of Military Assistance to Civil Authorities (MACA) and Military Support to Civil Authorities (MSCA), DOD uses DSCA as an emerging and overarching civil support term. DSCA refers to DOD support of civil authorities for domestic emergencies, and for designated law enforcement and other activities.

[64] Congressional Research Service, *Homeland Security: The Department of Defense's Role* RL 31615, 9; and, Department of Defense, *Report to Congress on The Role of the Department of Defense in Supporting Homeland Security*, 8.
[65] Department of Defense, *Report to Congress on The Role of the Department of Defense in Supporting Homeland Security*, (Washington, D.C., September 2003), 6.
[66] Ibid., 7.

Defense support is a very complex functional entity and requires broad cooperation with Federal, state, and local elements. DOD will normally provide support only when other local, state or Federal resources are unavailable and only if Defense support does not interfere with DOD's primary mission or ability to respond to operational contingencies.

The primary focus of intelligence collection and analysis within the DOD is on the foreign threat and on the generation of intelligence for the protection of U.S. forces at home and abroad. Terrorism that targets the homeland is fundamentally a law enforcement requirement best addressed by domestic law enforcement organizations. DOD may have a supporting role during crises. DOD has a responsibility to protect its forces, capabilities, and infrastructure within the United States. Along with Service and DOD law enforcement/counterintelligence organizations and USNORTHCOM, many Federal, state, and local organizations outside DOD have significant roles in collecting and analyzing information and intelligence, and in conducting investigations and operations to prevent or preempt terrorist attacks.

The traditional military assistance to civilian authorities (MACA)[67] encompasses military support to civil authorities (MSCA),[68] military assistance for civil disturbances (MACDIS),[69] and military assistance to law enforcement agencies (MACLEA). Assistance and support include capabilities for immediate response, loan of materiel, and people with subject matter expertise in functional emergency support. Military support to civilian authorities may also take the form of providing technical support and assistance to law enforcement, assisting in the restoration of law and order, providing specialized equipment, and assisting in consequence management.[70] If approved by the Secretary of defense, DOD designates a combatant commander for the response.[71]

Two circumstances exist for DOD providing Defense Support to Civil Authorities:

- In emergency circumstances, such as managing the consequences of a terrorist attack, major disaster, or other emergency, DOD could be asked to act quickly to provide capabilities that other agencies do not possess or that have been exhausted or overwhelmed.

- In non-emergency circumstances of limited scope or planned duration, DOD could be tasked to plan for and support civil authorities where other Federal agencies have the lead – for example, providing security at a special event such as the Olympics, or assisting other Federal agencies to develop capabilities to detect chemical, biological, nuclear, and radiological threats.

---

[67] DOD Directive 3025.15, *Military Assistance to Civil Authorities*, 18 February 1997.
[68] DOD Directive 3025.1, *Military Support to Civil Authorities (MSCA)*, 15 January 1993.
[69] DOD Directive 3025.12, *Military Assistance for Civil Disturbances (MACDIS)*, 4 February 1994.
[70] *National Strategy for Homeland Security*, 44.
[71] *National Response Plan*, Dec 2005, 42.

Civil support missions are supported by DOD when involvement is appropriate and when a clear end state for DOD participation is defined. DOD will seek reimbursement for civil support missions when authorized by U.S. law. Representative examples of DOD support of civil authorities are: DOD support to the Federal Bureau of Investigation (FBI) for incident management, law enforcement, intelligence support, and domestic counter terrorism activities; DOD support to the U.S. Coast Guard, including surveillance, patrol, and escort in the maritime domain and specialized support, such as Explosive Ordnance Disposal (EOD), Mine Countermeasures (MCM), and intelligence; or DOD support to the Department of Homeland Security (DHS), including support for domestic consequence management in the event of a chemical, biological, radiological, nuclear, or high-yield explosive terrorist attack.

Under the provisions of the Stafford Act, DOD support for disaster relief must be requested. (The other principal statute under which DOD provides emergency support is the Economy Act, under which any Federal agency can request support on a reimbursable basis from DOD.) Prior to appointment of a Defense Coordinating Officer (DCO), requests for Defense support are made through the Department of Defense Executive Secretary within the Office of the Secretary of Defense.

Defense Coordinating Officer (DCO)

Following appointment of a DCO, all requests for Defense support at the incident site management location are processed through the DCO. A Defense Coordinating Element (DCE) provides logistical and administrative support to the DCO. The DCO serves as *the single point of contact* at an incident site for coordinating and validating the use of DOD resources.[72] The DCO will collocate with the PFO or FCO in the Joint Field Office within the JFO Coordination Staff.[73]

Upon execution of the NRP, requests for Defense support must be accompanied by an Assistance Request Form (ARF) [a previous form had been titled a Request for Federal Assistance (RFA) form], unless the DOD component is responding under its independent funding authority or the commander's immediate response authority as defined in DOD Directive 3025.1. Some exceptions exist in requesting Defense Support to Civil Authorities such as Army Corps of Engineers (ACE) support, National Guard forces operating in State Active Duty or U.S. Title 32 status, or DOD forces in support of the FBI.[74] An authorizing official of the requesting agency validates and submits a request for assistance along with a fund cite.

Once the DCO validates the request, the DCE forwards the request directly to the supported combatant commander, or to the supporting headquarters designated by the combatant commander for execution. At times DOD provides, through the combatant commander, a joint task force (JTF) for command and control of DOD military forces. In this case, the DCO will normally work for the JTF commander as a special staff officer

[72] *National Response Plan*, Dec 2005, 42.
[73] Ibid., 37.
[74] Ibid., 42.

and closely coordinate with the task force operations section. The JTF commander exercises operational control of all allocated DOD resources (excluding USACE resources, National Guard forces operating in State Active Duty or Title 32 status, and in some instances, DD forces in support of the FBI.[75] The DCO remains the focal point in the Joint Field Office for requests for military support from the PFO or FCO, and after validation by the FRC or FCO, passes the requests to the JTF staff or other DOD organizations.

Defense Coordinating Officer (DCO)

- **Act as the designated DOD on-scene representative at JFO.**
- **Act as the DOD single point of contact (POC) at the incident management location for coordinating and processing requests for military support assistance by DOD.**
- **Coordinate request for assistance [Assistance Request Form ARF] and mission assignments with the FCO or designated Federal representative.**
- **Operate as DCO/DCE within the Joint Field Office (JFO).**
- **Direct on-scene support of Defense Coordinating Element (DCE), comprised of administrative staff and liaison personnel, including Emergency Preparedness Liaison Officers (EPLO).**
- **Forward mission assignments to appropriate military organizations through DOD-designated channels.**
- **Assign military liaisons, as appropriate, to activated Emergency Support Functions (ESF).**

Figure IV-1. **Defense Coordinating Officer**
(*Source*: National Response Plan, Dec 2005, 37and 42, and JHM)

DOD has a variety of relationships with state and local governments independent of those between state National Guard forces and DOD. The Army, Navy, Air Force, and Marine Corps Reserves provide Emergency Preparedness Liaison Officers (EPLO) to state and regional emergency response operations. The Emergency Preparedness Liaison Officer (EPLO) Program establishes liaison officers and support personnel in each state, with

[75] *National Response Plan*, Dec 2005, 42.
[77] Department of Defense, *Report to Congress on The Role of the Department of Defense in Supporting Homeland Security*, 15.

duty at the Governor's respective Department of Military Affairs or State Department of Defense, under the States' Adjutant Generals to coordinate mutual DOD support for national security emergency preparedness, response to natural or man-made disasters, and other domestic emergencies.[77]

On a case-by-case basis, people, units, equipment, and other DOD resources can be ordered to support a civil emergency; however, reservists cannot be ordered involuntarily to active duty solely to respond to a civil emergency except for extraordinary authorized circumstances in response to a CBRNE event.[78]

Army and Air National Guard forces, acting under state authority of the Governor (that is, not in Federal service), have primary responsibility for providing military assistance to state and local government agencies in civil emergencies within their respective states. The Guard includes highly specialized capabilities such as those provided by the state-controlled Weapons of Mass Destruction Civil Support Teams (WMD-CST). When such units, or other National Guard units and personnel, are directed to Federal service (Title 10 duty), they will respond to requirements validated by the designated DOD Defense Coordinating Officer.

Each DOD active and reserve installation maintains a relationship with local authorities from surrounding jurisdictions by virtue of proximity and their authority to provide immediate response. As DOD policy, a DOD installation commander may take immediate action to assist civil authorities or the public to save lives, prevent human suffering, or mitigate significant property damage under many imminently serious conditions that occur where there has been insufficient time to obtain approval through the chain of command and there has not been any declaration of major disaster or emergency by the U.S. President.

Installation commanders support area community relations with the local governments in order to address local security issues. DOD often participates in state-sponsored councils that focus on specific homeland security issues. USNORTHCOM works with both the regional and state-level Emergency Preparedness Offices to coordinate capabilities, plans, and operations. USNORTHCOM also includes state and regional level emergency response organizations in training activities and homeland defense exercises.[79]

Responsibilities of the DCO can be modified based on specific situations; however, normal functions include validating requests for Defense support and forwarding mission assignments to an appropriate military organization; and assigning military liaison officers to provide technical assistance to applicable activated Emergency Support

[78] Army War College, *How The Army Runs; A Senior Leader Reference Handbook 2005-2006*, U.S. Army War College, (Carlisle, PA: Department of Command, Leadership, and Management,), Final Coordinating Draft, 13 July 2005; Chapter 23; to be available at http://carlisle-ww.army.mil/usawc/dclm; Internet; August 2005.
[79] Department of Defense, *Report to Congress on The Role of the Department of Defense in Supporting Homeland Security*, 15.

Functions (ESF). The DCO, through appropriate military channels, refers contentious Defense support issues to the Assistant Secretary of Defense for Homeland Defense.[80]

DOD Authority

The Secretary of Defense maintains authority over DOD and conducts his responsibility in the chain of command for employing DOD forces under a military command and control system. The Secretary of Defense provides authorized and appropriate Defense support to civil authorities for domestic incidents, as directed by the President, or when consistent with military readiness and appropriate under the circumstances and the law. The chain of command for military forces providing Defense support of civil authorities remains constant and unchanged. Command for military forces is a direct link from the President, to the Secretary of Defense, to the Commander of a combatant command and to a joint task force. As one of several examples, USNORTHCOM has command over the commander of Joint Task Force Civil Support.

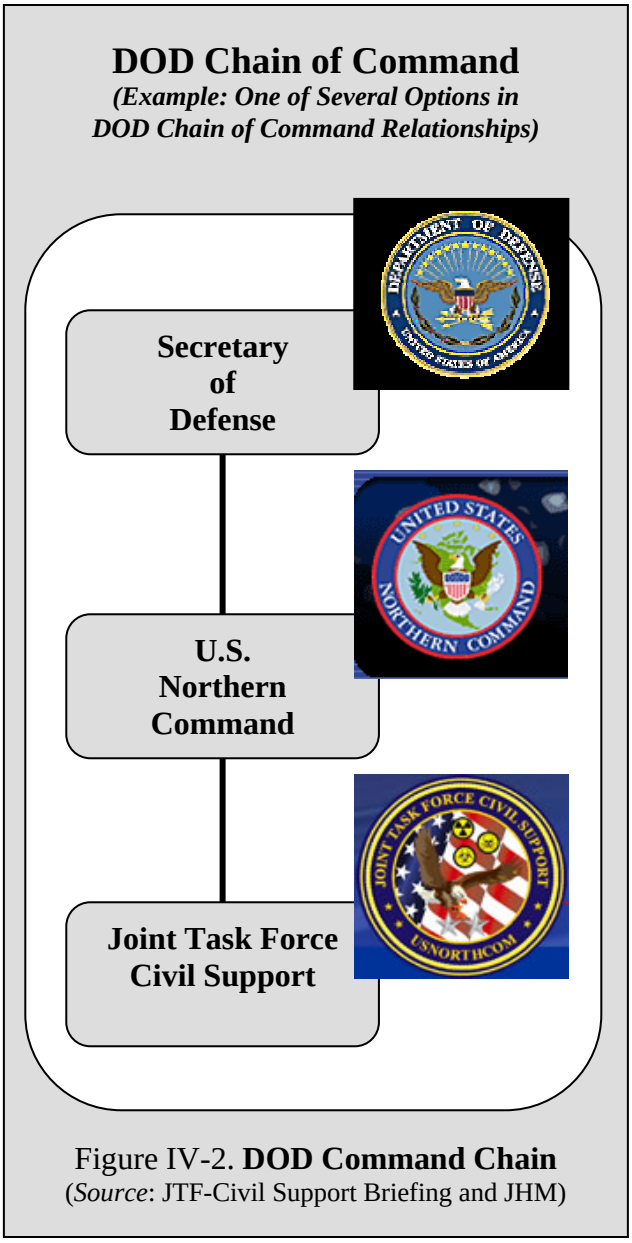

Figure IV-2. **DOD Command Chain**
(*Source*: JTF-Civil Support Briefing and JHM)

Accordingly, the civilian "unified command" concept used widely by civil public safety authorities as part of the emergency response and the Incident Command System (ICS) is distinct from the military chain of command. The Secretary of Defense retains command authority of military forces under DSCA.[81]

For terrorist incidents, the primary responsibilities for coordinating and conducting all Federal law enforcement and criminal investigation activities are executed by the Attorney General acting through the Federal Bureau of Investigation (FBI). During a terrorist incident, the local FBI Senior Agent in Charge

[80] *National Response Plan*, Dec 2005, 42.
[81] Ibid., 10.

(SAC) coordinates these activities with other members of the law enforcement community, and works in conjunction with the PFO, who coordinates the overall Federal incident management activities.[82]

At the strategic level of FBI operations, a Strategic Information Operations Center (SIOC) acts as the focal point and operational control center for all Federal intelligence, law enforcement, and investigative law enforcement activities related to a domestic terrorist incident or credible threats. The SIOC acts as an information clearing house to help collect, process, vet, and disseminate information relevant to law enforcement and criminal investigation efforts in a timely manner. The SIOC maintains direct connectivity to the Homeland Security Operation Center (HSOC) and the Interagency Incident Management Group (IIMG) for Federal headquarters-level multi-agency coordination, situational awareness, and incident management.[83]

U.S. Northern Command (USNORTHCOM)

A 2002 revision of the U.S. Unified Command Plan (UCP) established a new combatant command, U.S. Northern Command. USNORTHCOM is responsible for homeland defense and for assisting civil authorities in accordance with U.S. law. The commander of USNORTHCOM receives all operational orders from the U.S. President, through the Secretary of Defense.[84]

The Army maintains forces on a graduated response posture ready to support homeland defense missions. The Army also identifies multiple units ready to provide consequence management augmentation for Joint Task Force Civil Support, if required and directed by the Secretary of Defense. The Army continues to identify units ready to support the DOD Civil Disturbance Plan should that be required and directed by the Secretary of Defense.[85] The Army, in collaboration with the Air Force, is also developing enhanced capabilities to protect sites within the homeland from air attack. Additionally, the U.S. Navy works in conjunction with the U.S. Coast Guard to provide protection from maritime attacks.

U.S. Northern Command takes the homeland defense missions being performed by other Department of Defense organizations and places them within a single combatant command. Simultaneously, U.S. Northern Command plans, organizes, and executes civil support missions.

The USNORTHCOM mission is homeland defense and civil support. Specifically, this combatant command:

- Conducts operations to deter, prevent, and defeat threats and aggression aimed at the United States, its territories, and interests within the assigned area of responsibility.

[82] Ibid., 16.
[83] Ibid., 22, 24, and 26.
[84] *National Strategy for Homeland Security*, 44 and 45.
[85] Department of Defense, *Report to Congress on The Role of the Department of Defense in Supporting Homeland Security*, 5.

- As directed by the President or Secretary of Defense, provides military assistance to civil authorities including consequence management operations.

The diagram at Figure 1-11 shows the main types of task force elements that may comprise a Joint Task Force with a consequence management mission. USNORTHCOM employs a flexible tiered response concept of operations. Military support will be tailored to the scope and magnitude of the situation and will be focused on capabilities to meet the response requirements beyond the resources of civil authorities. The appropriate CBRNE consequence management command and control (C2) headquarters is determined based on size and complexity of the DOD required response, in accordance with a flexible tiered response concept. This notional illustration for a response incident presents four main elements: site support, medical support, logistical support, and support for the JTF headquarters.

Notional Joint Task Force for Consequence Management

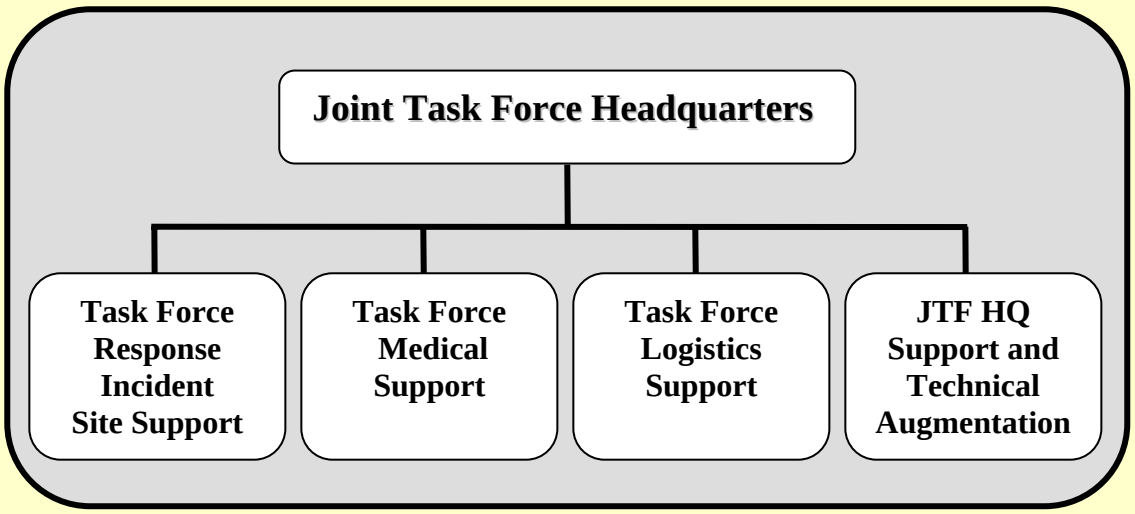

Figure IV-3. **Notional Joint Task Force for Consequence Management**
(*Source:* JTF-Civil Support J5 2005 and JHM)

Reserve Components

The relationship between the DOD, including its combatant commands, and the National Guard and Reserve is clearly defined by law with respect to homeland security and homeland defense roles. In cases where the governors of the states and territories employ National Guard forces in a state status to perform state missions of a homeland security nature, those National Guard forces have no direct operational relationship to the Department or its combatant commands. However, the National Guard and Reserve

components represent the nation's strategic reserve of organized military capability, and are critical to DOD ability to sustain long-term military operations.

National Guard personnel serving in a State Active Duty or Title 32 status remain subject to recall to active duty under Title 10 to meet Federal requirements. The Chairman, Joint Chiefs of Staff, maintains visibility of National Guard assets performing homeland security missions, as do combatant commanders in order to adjust warfighting plans if necessary to overcome reductions in assigned capabilities. Moreover, USNORTHCOM and PACOM must have visibility of state controlled National Guard operations to facilitate coordination between Title 10 and Title 32 or State Active Duty military operations, which might be occurring in the same area, at the same time, towards a common objective.[86]

Federal Military Forces and U.S. Law

The USNORTHCOM homeland defense mission is directed against military threats emanating from outside the United States. USNORTHCOM has a cooperative relationship with Federal agencies working to prevent terrorism. These organizations share information and work together to coordinate plans and actions. This level of cooperation and information sharing improves the effectiveness of homeland security efforts overall and enhances prevention of threats, attacks and other acts of aggression against the United States. Notwithstanding, many organizations at local, state and Federal levels have important roles in collecting intelligence, investigating, and then conducting the operations to preempt terrorism. The *Posse Comitatus Act*[87] prevents the Federal U.S. military from direct law enforcement involvement.

A significant difference between homeland security and homeland defense is the limitations on use of Federal military forces. USNORTHCOM is a military organization whose operations within the United States are governed by Federal law that prohibits direct military involvement in law enforcement activities. DOD and USNORTHCOM roles in support of homeland security are limited to homeland defense and civil support.

Terrorism targeted against the United States is fundamentally a homeland security matter usually addressed by law enforcement agencies. The National Strategy for Homeland Security defines homeland security as a concerted national effort to prevent terrorist attacks with the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. Homeland defense (HLD) is the protection of U.S. territory, domestic population and critical infrastructure against military attacks emanating from outside the United States.

---

[86] Ibid., 15 and 16.

[87] The *Posse Comitatus Act*, 18 U.S.C. 1385, prohibits the use of the Army or the Air Force for law enforcement purposes, except as otherwise authorized by the Constitution or statute. This prohibition applies to Navy and Marine Corps personnel as a matter of DOD policy. The primary prohibition of the *Posse Comitatus Act* is against direct involvement by active duty military personnel (to include Reservists on active duty and National Guard personnel in Federal service) in traditional law enforcement activities (to include interdiction of vehicle, vessel, aircraft, or other similar activity; a search or seizure; an arrest, apprehension, stop and frisk, or similar activity).

Section V: Defending Against WMD/E Threats - CBRNE

The United States of America is the world's fourth largest nation with 3.5 million square miles of land and 88,000 miles of tidal shoreline. Each year, 11.2 million trucks and 2.2 million rail cars cross into the U.S. from the 7,500-mile land and air border shared with Canada and Mexico. Over 7,500 foreign-flag ships make 51,000 calls annually to U.S. ports. The country routinely admits millions of visitors from around the world.[88]

Underlying these social, economic, and political arenas, ruthless and resourceful terrorists seek to threaten the U.S. with new technologies, dangerous weapons, and nontraditional tactics that exploit our freedoms. As the nation witnessed on September 11, 2001, enemies of the U.S. have the resolve and means to commit acts of terrorism and mass destruction against innocent civilians and commercial interests within our country.

Having few permanently assigned forces, USNORTHCOM will be assigned forces whenever necessary to execute missions as ordered by the President and as provided by the U.S. Armed Services. Yet, several pre-existing joint force headquarters have been assigned to USNORTHCOM with the ability to execute missions such as counterdrug assistance, homeland security, homeland defense, and civil support for CBRNE consequence management on a daily basis.

An Army mission is to support disaster assistance and other civil programs.[89] With the establishment of USNORTHCOM, the Commander of U.S. Forces Command (USFORSCOM) serves in the role of the Army Service Component Commander for USNORTHCOM. Headquarters, USFORSCOM retains its role as a force provider and remains assigned to U.S. Joint Forces Command (JFCOM).[90]

USFORSCOM is U.S. Northern Command's coordinating authority for Defense Support to Civil Authorities (DSCA) and supports domestic emergencies through its two Continental U.S. Army (CONUSA) headquarters. DSCA command and control relationships are changing for designated mission support by each CONUSA to USFORSCOM and USNORTHCOM. Both First Army and Fifth Army have assigned areas of responsibility that approximate the eastern and western half of the USA with specified additions. U.S. Pacific Command (USPACOM) provides MACA within its extensive assigned area of responsibility.[91]

The Armed Services provide increased homeland security and disaster response capabilities to the U.S. in support of the charter of the Department of Homeland Security. Ground, air, space, and maritime areas of interest align Army, Navy, Air Force, and Marine Corps capabilities to support governmental programs such as air defense, inland

[88] USNORTHCOM [U.S. Northern Command] website; available at http://www.northcom.mil; Internet; accessed 28 April 2004.
[89] Army Field Manual FM1, *The Army*, 14 June 2005, 2-6.
[90] Department of Defense, *Report to Congress on The Role of the Department of Defense in Supporting Homeland Security*, 6.
[91] Army War College, *How The Army Runs: A Senior Leader Reference Handbook 2003-2004*, 474.

waterways, port facilities, and border and critical infrastructure security. One example of a specific disaster response asset is the Marine Corps' Chemical, Biological Incident Response Force (CBIRF) and other Marine Corps assets. Tasks include detecting terrorist actions, deterring terrorist acts, defending specified locations, and conducting initial incident response to chemical, biological, radiological, or nuclear terrorist attacks.[92]

The specter for weapons of mass destruction is a range of capabilities spanning chemical, biological, radiological, nuclear, and high yield explosives (CBRNE). Incidents that may cause catastrophic damage and destruction include industrial accidents, acts of nature, acts of war, and terrorism. Effective CBRNE response requires a distinct and deliberate set of resources, skills and experience.

Understanding Joint Task Force - Civil Support

The purpose of Joint Task Force Civil Support is to save lives, prevent injury and provide temporary critical life support during a chemical, biological, radiological, nuclear or high-yield explosive (CBRNE) situation in the United States or its territories and possessions. JTF-Civil Support is the only U.S. military organization dedicated solely to planning and integrating Department of Defense forces for consequence management (CM) support to civil authorities.

As a standing joint task force headquarters, JTF-Civil Support comprises active component, reserve component and National Guard members from the Army, Navy, Air Force, Marines and Coast Guard, as well as civilian personnel, and is commanded by a federalized Army National Guard General Officer. The joint task force stands ready to aid the designated lead agency, most likely the Federal Emergency Management Agency (FEMA), in charge of managing the consequences of a CBRNE accident or incident. A former independent agency tasked with planning for and responding to disasters, FEMA is now a part of the Department of Homeland Security.

When directed by the Commander of U.S. Northern Command, JTF-Civil Support will deploy to the incident site, establish command and control of designated DOD forces, and provide military assistance to civil authorities to save lives, prevent injury and provide temporary critical life support in order to reduce the harmful effects of a CBRNE incident.

Within its USNORTHCOM Charter, JTF-Civil Support is a standing Joint Task Force headquarters under the combatant command (COCOM)[93] of Commander,

[92] Department of Defense, *Report to Congress on The Role of the Department of Defense in Supporting Homeland Security*, 5 to 8.

[93] Combatant Command (Command Authority) (COCOM). (DOD) Nontransferable command authority established by title 10 ("Armed Forces"), United States Code, section 164, exercised only by commanders of unified or specified combatant commands unless otherwise directed by the President or the Secretary of Defense. Combatant command (command authority) cannot be delegated and is the authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Operational control is inherent in combatant command (command

USNORTHCOM, and is authorized several command relationships. USNORTHCOM is the Supported Combatant Commander within its area of responsibility (AOR) and will normally maintain both administrative control (ADCON)[94] and operational control (OPCON)[95] of JTF-Civil Support. During domestic situations in the USPACOM AOR, USNORTHCOM will be a Supporting Combatant Commander and, when directed by the SECDEF, will transfer OPCON of JTF-Civil Support to the Supported Combatant Commander. Subordinate units or elements of JTF-Civil Support will normally be either attached,[96] OPCON, or TACON[97] for command or control to the Commander of JTF-Civil Support by USNORTHCOM to accomplish mission tasks.

The Commander of JTF-Civil Support, when directed, will exercise OPCON over the Defense Coordinating Officer (DCO) and the Defense Coordinating Element (DCE) during a CBRNE situation. Located in the Joint Field Office, the DCO works closely with the Federal Coordinating Officer (FCO) or other senior DHS (FEMA) officials on the scene.

When coordinated by USNORTHCOM, the Commander JTF-Civil Support is granted Direct Liaison Authorized (DIRLAUTH) with designated Initial Entry Force (IEF) units for CBRNE CM information sharing, exercise and operational planning, and interoperability issues. DIRLAUTH and coordination does not include tasking authority unless OPCON or TACON of tasked forces is specifically authorized. DIRLAUTH is authorized with other DOD CBRNE CM capable units and Defense agencies to enhance operational planning.[98] Again, DIRLAUTH and coordination does not include tasking authority unless OPCON or TACON of the tasked forces is specifically authorized.

---

authority). (JP 1-02); available at http://www.au.af.mil/au/awc/awcgate/pub1/appendix_g.pdf; Internet; accessed 26 May 2004.

[94] Administrative Control (ADCON). (DOD) Direction or exercise of authority over subordinate or other organizations in respect to administration and support, including organization of Service forces, control of resources and equipment, personnel management, unit logistics, individual and unit training, readiness, mobilization, demobilization, discipline, and other matters not included in the operational missions of the subordinate or other organizations. (JP 1-02)

[95] Operational Control (OPCON). (DOD) Transferable command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational control may be delegated and is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. (JP 1-02)

[96] Attach. (DOD) 1. The placement of units or personnel in an organization where such placement is relatively temporary. 2. The detailing of individuals to specific functions where such functions are secondary or relatively temporary, e.g., attached for quarters and rations; attached for flying duty. (JP 1-02)

[97] Tactical Control (TACON). Command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed and, usually, local direction and control of movements or maneuvers necessary to accomplish missions or tasks assigned. Tactical control is inherent in operational control. Tactical control may be delegated to, and exercised at any level at or below the level of combatant command. See also combatant command; combatant command (command authority); operational control. (JP 1-02)

[98] See CJCSI 3110.16, *Military Capabilities, Assets, and Units of CBRNE CM Operations*, for a sampling of DOD CBRNE consequence management type-units and agencies that may be configured in JTF-Civil Support.

Through the National Guard Bureau, the Commander JTF-Civil Support is granted DIRLAUTH with each state-level National Guard Joint Force Headquarters, to include National Guard Weapons of Mass Destruction-Civil Support Teams (WMD-CSTs), for coordination and planning that supports the overall military capabilities for CBRNE emergency response. The Commander JTF-Civil Support informs and updates USNORTHCOM, Service Component Headquarters, the Chief of the National Guard Bureau, and The state Adjutants General (TAGs) of ongoing coordination, planning, and actions.

The primary mission authority allowing DOD to engage in domestic consequence management operations is the Robert T. Stafford Disaster Relief and Emergency Assistance Act. The Stafford Act authorizes the President to provide disaster and emergency assistance to state and local governments upon receipt of a request from a Governor. Deployment of JTF- Civil Support, at the direction of the Commander of U.S. Northern Command, and on the authority of the Secretary of Defense, would occur only after a Governor requests Federal assistance from the President, and after the President issues a Presidential Disaster Declaration.

Preparing for and executing a domestic consequence management mission requires JTF-Civil Support to work closely with the many other Federal, state and local agencies that also respond to CBRNE situations. These agencies include, but are not limited to, the Department of Homeland Security's Federal Emergency Management Agency, the Department of Health and Human Services, and state emergency management agencies. DOD is an essential member of the Federal response community and interagency preparedness.[99]

JTF-Civil Support Mission

The mission of JTF-Civil Support is to provide command and control for Department of Defense forces deployed in support of a Lead Federal Agency (LFA) managing the consequences of a chemical, biological, radiological, nuclear or high-yield explosive (CBRNE) incident in the United States, its territories and possessions, in order to save lives, prevent injury and provide temporary critical life support. JTF-Civil Support serves as a standing operational headquarters for USNORTHCOM.

The JTF-Civil Support mission includes, but is not limited to, the following range of activities:

- Conduct contingency planning with Federal departments and agencies.
- Conduct operational liaison activities with local, state and Federal departments and agencies.

[99] Joint Task Force – Civil Support [U.S. Northern Command] website; available at http://www.jtfcs.northcom.mil; Internet; accessed 14 April 2004.

- Conduct CBRNE CM exercises within DOD and with other local, state and Federal departments and agencies.

- Conduct CBRNE CM training and exercises with DOD forces identified to conduct CBRNE CM operations.

- Conduct situational assessments following CBRNE events for the Commander in close coordination with state and Federal authorities.

- Organize, deploy, establish command and control, and redeploy DOD assigned, attached, operationally or tactically controlled forces.

- Conduct deliberate planning in support of designated National Security Special Events (NSSEs).

- Organize and provide CBRNE consequence management planning augmentation and technical support as directed.

Page Intentionally Blank

Section VI: Conclusion – WMD/E Consequence Management

Terrorist groups are seeking to acquire WMD with the stated purpose of killing large numbers of U.S. citizens and U.S. friends and allies - without compunction and without warning.[100] The threat posed by terrorists with the intent to use weapons of mass destruction is ominous. WMD attack has several desired outcomes by terrorists. These expectations range from extensive disruption of everyday lifestyles to a more serious boding of massive damage to physical infrastructure, the economy, or mass casualties requiring long-term health care. Ultimately, a significant impact could be an intimidating psychological trauma from physical and emotional stress. Simply stated, the ***potential*** for mass injury or death, as well as mass damage or destruction, presents a compelling requirement for protective measures and increased assurance to counter public anxiety and fear.[101]

Defined in U.S. Title 18, a *Weapon of Mass Destruction (WMD)* is (1) any explosive, incendiary, or poison gas, bomb, grenade, rocket having a propellant charge of more than four ounces, or a missile having an explosive or incendiary charge of more than one quarter ounce, or mine or device similar; (2) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors; (3) any weapon involving a disease organism; or (4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life.

> **"The gravest danger our Nation faces lie at the crossroads of radicalism and technology. Our enemies have openly declared that they are seeking weapons of mass destruction, and evidence indicates that they are doing so with determination. The United States will not allow these efforts to succeed.... History will judge harshly those who saw this coming danger but failed to act. In the new world we have entered, the only path to peace and security is the path of action."**
>
> George W. Bush
> The President of the United States of America
> September 17, 2002

Current and potential linkages among terrorist groups and state sponsors of terrorism are particularly dangerous and require priority attention. Catastrophic incidents with

[100] HSPD-17, 1.
[101] Steven Bowman, *Weapons of Mass Destruction: The Terrorist Threat,* Congressional Research Service Report for Congress, CRS Order Code RL31332, 7 March 2002; available from http://www.fas.org/irp/crs/RL31332.pdf; Internet; accessed 15 April 2004.

CBRNE, including terrorism, will result in unprecedented levels of damage and disruption severely affecting the population, infrastructure, environment, and economy. The aftermath of such a catastrophic event would result in sustained national impacts over a prolonged period of time. Consequence management is essential to the U.S. arsenal bearing against the WMD terrorist threat.[102]

Three principal pillars summarize the U.S. *National Strategy to Combat Weapons of Mass Destruction*: (1) counterproliferation to combat WMD use; (2) strengthened nonproliferation to combat WMD proliferation; and (3) consequence management to respond to a WMD incident. The U.S. Government is prepared to deal with the consequences of chemical, biological, radiological, or nuclear weapon use within and outside of the United States.[103] The Department of Defense remains the greatest U.S. Federal repository of resources and subject matter expertise for responding to a chemical, biological, radiological, or nuclear incident.[104] The growing pattern of high yield explosive use adds to a macabre inventory of a terrorist bent on mass destruction effects.

As witnessed after the events of 9-11, DOD will most likely be involved in consequence management operations following a significant terrorist attack on the United States. Especially those attacks that include CBRNE.

Joint Task Force Civil Support is a ready expression of U.S. capability to respond to such incidents of chemical, biological, radiological, nuclear, and high yield explosives (CBRNE).

[102] *HSPD-17*, 7.
[103] Ibid., 6.
[104] Congressional Research Service, *Homeland Security: The Department of Defense's Role*, CRS Order Code RL 31615, 8.

Glossary

anti-terrorism: (AT) (JP 1-02) — Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces.

AOR: Area of Responsibility

asset (terrorist): A resource — person, group, relationship, instrument, installation, or supply — at the disposition of a terrorist organization for use in an operational or support role. Often used with a qualifying term such as suicide asset or surveillance asset. Based upon JP 1-02 asset (intelligence).

biological agent: (JP 1-02) — A microorganism that causes disease in personnel, plants, or animals or causes the deterioration of materiel.

biological weapon: (JP 1-02) — An item of materiel, which projects, disperses, or disseminates a biological agent including arthropod vectors.

bioregulators: (CBRN Handbook) Biochemicals that regulate bodily functions. Bioregulators that are produced by the body are termed "endogenous." Some of these same bioregulators can be chemically synthesized.

blister agents: (CBRN Handbook) Substances that cause blistering of the skin. Exposure is through liquid or vapor contact with any exposed tissue (eyes, skin, lungs).

blood agents: (CBRN Handbook) Substances that injure a person by interfering with cell respiration (the exchange of oxygen and carbon dioxide between blood and tissues).

CBIRF: Chemical-Biological Incident Response Force.

CBRNE: Chemical, biological, radiological, nuclear, and high yield explosive categories normally associated with weapons of mass destruction.

chemical weapon: (JP 1-02) — Together or separately, (a) a toxic chemical and its precursors, except when intended for a purpose not prohibited under the Chemical Weapons Convention; (b) a munition or device, specifically designed to cause death or other harm through toxic properties of those chemicals specified in (a), above, which would be released as a result of the employment of such munition or device; (c) any equipment specifically designed for use directly in connection with the employment of munitions or devices specified in (b) above.

chemical agent: (CBRN Handbook) A chemical substance that is intended for use in military operations to kill, seriously injure, or incapacitate people through its physiological effects. Excluded from consideration are riot control agents, and smoke and flame materials. The agent may appear as a vapor, aerosol, or liquid; it can be either a casualty/toxic agent or an incapacitating agent.

choking agents: (CBRN Handbook) Substances that cause physical injury to the lungs. Exposure is through inhalation. In extreme cases, membranes swell and lungs become filled with liquid. Death results from lack of oxygen; hence, the victim is "choked."

conflict: (Army) — A political-military situation between peace and war, distinguished from peace by the introduction of organized political violence and from war by its reliance on political methods. It shares many of the goals and characteristics of war, including the destruction of governments and the control of territory. See FM 100-20.

COCOM: Combatant command, that is, command authority. See page 247 footnote of handbook. (JP 1-02)

consequence management: Traditionally, consequence management has been predominantly an emergency management function and included measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism. The requirements of consequence management and crisis management are combined in the NRP.

CONUS: Continental United States

counter-terrorism: (CT) Offensive measures taken to prevent, deter, and respond to terrorism.

crisis management: Traditionally, crisis management was predominantly a law enforcement function and included measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism. The requirements of consequence management and crisis management are combined in the NRP.

cyber-terrorism: (FBI) — A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda.

Defense Coordinating Officer: (DCO) The single point of contact at an incident management location for coordinating and validating the use of DOD resources. DCO works directly with the FCO or designated Federal representative, and coordinates request for assistance with the joint force commander, when a JTF is tasked to an incident response. See NRP.

Defense Information System Network: (DISN) The global, end-to-end information transfer infrastructure of DOD. It provides long haul data, voice, video, and transport networks and services needed for national defense command, control, communication, and intelligence requirements, as well as corporate defense requirements.

DSWA: Defense Special Weapons Agency

Defense Support of Civil Authorities: (DSCA) An emergent term under consideration for inclusion to the 2004 National Response Plan that incorporates the Department of Defense support to domestic emergencies, law enforcement, and other activities. A traditional overarching term is Military Assistance to Civil Authorities (MACA) which includes Military Support to Civil Authorities (MSCA) and Military Assistance to Law Enforcement (MACLEA). See NRP.

Designated Foreign Terrorist Organization: (DFTO) A political designation determined by the U.S. Department of State. Listing as a DFTO imposes legal penalties for membership, prevents travel into the U.S., and proscribes assistance and funding activities within the U.S. or by U.S. citizens. From Patterns of Global Terrorism 2001, U.S. Department of State.

DIRLAUTH: Direct liaison authorized

DHS: Department of Homeland Security

Domestic Emergency Support Team: (DEST) See NRP.

Emergency Response Team: (ERT) See NRP.

Emergency Support Functions: (ESF) See NRP.

EPLO: Emergency Preparedness Liaison Officer. See NRP.

failed state: For the purposes of this circular, a dysfunctional state which also has multiple competing political factions in conflict within its borders, or has no functioning governance above the local level. This does not imply that a central government facing an insurgency is automatically a failed state. If essential functions of government continue in areas controlled by the central authority, it has not "failed."

Federal Coordinating Officer: (FCO) A Federal representative who manages Federal resource support activities related to Stafford Act disasters and emergencies; supports and is subordinate to the Principle Federal Official (PFO) when one is designated by DHS.

Federal Incident Response Support Team: (FIRST) See NRP.

FEMA: Federal Emergency Management Agency. See NRP.

force protection: Security program designed to protect Service members, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and other security programs.

force protection condition (FPCON): There is a graduated series of Force Protection Conditions ranging from Force Protection Conditions Normal to Force Protection Conditions Delta. There is a process by which commanders at all levels can raise or lower the Force Protection Conditions based on local conditions, specific threat information and/or guidance from higher headquarters. The four Force Protection Conditions above normal are:

Force Protection Condition ALPHA --This condition applies when there is a general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of Force Protection Conditions BRAVO measures. The measures in this Force Protection Conditions must be capable of being maintained indefinitely.

Force Protection Condition BRAVO --This condition applies when an increased and more predictable threat of terrorist activity exists. The measures in this Force Protection Conditions must be capable of being maintained for weeks without causing undue hardship, affecting operational capability, and aggravating relations with local authorities.

Force Protection Condition CHARLIE --This condition applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and facilities is imminent. Implementation of measures in this Force Protection Conditions for more than a short period probably will create hardship and affect the peacetime activities of the unit and its personnel.

Force Protection Condition DELTA --This condition applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is likely. Normally, this Force Protection Conditions is declared as a localized condition.

FRC: Federal Resource Coordinator. See NRP.

guerrilla warfare: (JP 1-02, NATO) — Military and paramilitary operations conducted in enemy-held or hostile territory by irregular, predominantly indigenous forces. (See also unconventional warfare (UW).

GWOT: Global War on Terrorism.

HD: Homeland Defense.

HLD: Homeland Defense.

HS: Homeland Security.

Homeland Security Advisory System (HSAS): The advisory system provides measures to remain vigilant, prepared, and ready to deter terrorist attacks. The following Threat Conditions each represent an increasing risk of terrorist attacks. Beneath each Threat Condition are suggested protective measures, recognizing that the heads of Federal departments and agencies are responsible for developing and implementing appropriate agency-specific protective measures:

- **Low Condition (Green)**. This condition is declared when there is a low risk of terrorist attacks. Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures they develop and implement: refining and exercising as appropriate preplanned Protective Measures; ensuring personnel receive proper training on the Homeland Security Advisory System and specific preplanned department or agency Protective Measures; and institutionalizing a process to assure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks, and all reasonable measures are taken to mitigate these vulnerabilities.

- **Guarded Condition (Blue)**. This condition is declared when there is a general risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Condition, Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement: checking communications with designated emergency response or command locations; reviewing and updating emergency response procedures; and providing the public with any information that would strengthen its ability to act appropriately.

- **Elevated Condition (Yellow)**. An Elevated Condition is declared when there is a significant risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the Protective Measures that they will develop and implement: increasing surveillance of critical locations; coordinating emergency plans as appropriate with nearby jurisdictions; assessing whether the precise characteristics of the threat require the further refinement of preplanned Protective Measures; and implementing, as appropriate, contingency and emergency response plans.

- **High Condition (Orange)**. A High Condition is declared when there is a high risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement: coordinating necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations; taking additional precautions at public events and possibly considering alternative venues or even cancellation; preparing to execute contingency procedures, such as moving to an alternate site or dispersing their workforce; and restricting threatened facility access to essential personnel only.

- **Severe Condition (Red)**. A Severe Condition reflects a severe risk of terrorist attacks. Under most circumstances, the Protective Measures for a Severe Condition are not intended to be sustained for substantial periods of time. In addition to the Protective Measures in the previous Threat Conditions, Federal departments and agencies also should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement: increasing or redirecting personnel to address critical emergency needs; signing emergency response personnel and pre-positioning and mobilizing specially trained teams or resources; monitoring, redirecting, or constraining transportation systems; and closing public and government facilities.

HSOC: Homeland Security Operations Center.

HSPD: Homeland Security Presidential Directive.

HUMINT: Human intelligence.

HYE: High Yield Explosive.

IED: Improvised Explosive Device. Devices that have been fabricated in an improvised manner and that incorporate explosives or destructive, lethal, noxious, pyrotechnic, or incendiary chemicals in their design.

IEF: Initial Entry Force.

IIMG: Interagency Incident Management Group.

incapacitating agent: (CBRN Handbook) Produce temporary physiological and/or mental effects via action on the central nervous system. Effects may persist for hours or days, but victims usually do not require medical treatment. However, such treatment speeds recovery.

Incident Command System (ICS): A standardized on-scene emergency management concept specifically designed to allow its user(s) to adopt an integrated organizational structure equal to the complexity and demands of single or multiple incidents without being hindered by jurisdictional boundaries. The national standard for ICS is provided by NIMS.

industrial agent: (CBRN Handbook) Chemicals developed or manufactured for use in industrial operations or research by industry, government, or academia. These chemicals are not primarily manufactured for the specific purpose of producing human casualties or rendering equipment, facilities, or areas dangerous for use by man. Hydrogen cyanide, cyanogen chloride, phosgene, chloropicrin and many herbicides and pesticides are industrial chemicals that also can be chemical agents.

insurgency: (JP 1-02, NATO) — An organized movement aimed at the overthrow of a constituted government through the use of subversion and armed conflict.

international: of, relating to, or affecting two or more nations (Webster's). For our purposes, affecting two or more nations.

Joint Field Office: (JFO) See National Response Plan.

Joint Operations Center: (JOC) See NRP.

JTF: Joint Task Force.

LFA: Lead Federal Agency.

millenarian: Apocalyptic; forecasting the ultimate destiny of the world; foreboding imminent disaster or final doom; wildly unrestrained; ultimately decisive. (Merriam –Webster's)

MACA: Military Assistance to Civil Authorities.

MACC: Multi-Agency Command Center.

MACDIS: Military Assistance for Civil Disturbances.

MACLEA: Military Assistance to Law Enforcement.

narco-terrorism: (JP 3-07.4) Terrorism conducted to further the aims of drug traffickers. It may include assassinations, extortion, hijackings, bombings, and kidnappings directed against judges, prosecutors, elected officials, or law enforcement agents, and general disruption of a legitimate government to divert attention from drug operations.

nation: A community of people composed of one or more nationalities and possessing a more or less defined territory and government or a territorial division containing a body of people of one or more nationalities and usually characterized by relatively large size and independent status.

nation-state: A form of political organization under which a relatively homogeneous people inhabits a sovereign state; especially a state containing one as opposed to several nationalities.

nerve agents: (CBRN Handbook) Substances that interfere with the central nervous system. Exposure is primarily through contact with the liquid (skin and eyes) and secondarily through inhalation of the vapor. Three distinct symptoms associated with nerve agents are: pin-point pupils, an extreme headache, and severe tightness in the chest.

National Incident Management System: (NIMS). See *National Incident Management System* published by the Department of Homeland Security, 1 March 2004. The NIMS represents a core set of doctrine, concepts, principles, technology and organizational processes to enable effective, efficient, and collaborative incident management. Nationwide context is an all-hazards, all jurisdictional levels, and multi-disciplines approach to incident management.

National Response Plan: (NRP) The *National Response Plan* (December 2004) is an all-discipline, all-hazards plan that establishes a single, comprehensive framework for the management of domestic incidents. It provides the structure and mechanisms for the coordination of Federal support to State, local, and tribal incident managers and for exercising direct Federal authorities ad responsibilities.

NORAD: North American Aerospace Defense Command.

NSSE: National Special Security Event.

nuclear weapon: (JP 1-02) — A complete assembly (i.e., implosion type, gun type, or thermonuclear type), in its intended ultimate configuration which, upon completion of the prescribed arming, fusing, and firing sequence, is capable of producing the intended nuclear reaction and release of energy.

OPCON: Operational control, that is, transferable command authority. See Appendix H of terrorism handbook. (JP 1-02).

operations security: (OPSEC) A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. Identify those actions that can be observed by adversary intelligence systems. b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. (Joint Pub 1-02)

Pathogen: (CBRN Handbook) Any organism (usually living) capable of producing serious disease or death, such as bacteria, fungi, and viruses

physical security: That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material and documents; and to safeguard them against espionage, sabotage, damage, and theft. (Joint Pub1-02)

POTUS: President of the United States.

Principle Federal Official: (PFO) Senior representative of Secretary of Homeland Security and lead Federal official on-scene to coordinate Federal domestic incidents management and resource allocation on-scene. See NRP.

Radiological Dispersal Device: (RDD) (CBRN Handbook) A device (weapon or equipment), other than a nuclear explosive device, designed to disseminate radioactive material in order to cause destruction, damage, or injury by means of the radiation produced by the decay of such material.

Radiological Emitting Device: (RED) A device designed to disseminate radioactive material in order to cause destruction, damage, or injury by means of the radiation produced by the decay of such material. RED dissemination techniques can include intense, short duration exposure or progressive, long-term exposure to radiation.

radiological operation: (JP 1-02) — The employment of radioactive materials or radiation producing devices to cause casualties or restrict the use of terrain. It includes the intentional employment of fallout from nuclear weapons.

RFA: Request for Federal Assistance.

SAC: Senior Agent in Charge. See NRP.

SCO: State Coordinating Officer. See NRP.

setback: Distance between outer perimeter and nearest point of buildings or structures within. Generally referred to in terms of explosive blast mitigation.

SFLEO: Senior Federal law Enforcement Officer. See NRP.

SFO: Senior Federal Official. See NRP.

state: A politically organized body of people usually occupying a definite territory; especially one that is sovereign.

TACON: Tactical control, that is, command authority with detailed limitations and responsibilities inherent to operational control. (JP 1-02).

terror tactics: Given that the Army defines tactics as **"**the art and science of employing available means to win battles and engagements," then terror tactics should be considered "the art and science of employing violence, terror and intimidation to inculcate fear in the pursuit of political, religious, or ideological goals."

terrorism: (JP 1-02) — The calculated use of violence or threat of 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.

terrorist: (JP 1-02) — An individual who uses violence, terror, and intimidation to achieve a result.

terrorist goals: The term *goals* will refer to the strategic end or end state that the terrorist objectives are intended to obtain.

terrorist group: Any group practicing, or that has significant subgroups that practice, international terrorism (U.S. Dept of State)

terrorist objectives: The standard definition of *objective* is – "The clearly defined, decisive, and attainable aims which every military operation should be directed towards" (JP 1-02). For the purposes of this work, terrorist objectives will refer to the intended outcome or result of one or a series of terrorist operations or actions.

toxic chemical agent: (CBRN Handbook) Produce incapacitation, serious injury, or death. They can be used to incapacitate or kill victims. These agents are the choking, blister, nerve, and blood agents.

toxin agent: (JP 1-02) **—** A poison formed as a specific secretion product in the metabolism of a vegetable or animal organism, as distinguished from inorganic poisons. Such poisons can also be manufactured by synthetic processes.

transnational: Extending or going beyond national boundaries (Webster's). In this context, not limited to or centered within a single nation.

unified command: As a term in the Federal application of the Incident Command System (ICS), defines agencies working together through their designated Incident Commanders at a single Incident Command Post (ICP) to establish a common set of objectives and strategies, and a single Incident Action Plan. This is NOT "unified command" as defined by the Department of Defense.

USACE: United States Army Corps of Engineers.

USNORTHCOM: U.S. Northern Command.

USSS: U.S. Secret Service

UXO: Unexploded ordnance

VBIED: Vehicle Borne Improvised Explosive Device

WOT: War on Terrorism

WEG: Worldwide Equipment Guide. A document produced by the TRADOC ADCSINT – Threats that provides the basic characteristics of selected equipment and weapons systems readily available for use by the OPFOR.

WMD: (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.

WMD-CST: Weapons of Mass Destruction – Civil Support Team

WMD/E: Weapons of mass destruction or effect is an emergent term referenced in the 2004 U.S. National Military Strategy to address a broader range of adversary capabilities with potentially devastating results.

Selected Bibliography

"April 1983 US Embassy bombing." Available from http://encyclopedia.thefreedictionary.com/April%2011983%20US%20Embassy%20bombing; Internet; Accessed 1 July 2004.

Albright, David. "Al Qaeda's Nuclear Program: Through the Window of Seized Documents." *Policy Forum Online* 47 (6 November 2002): 1-12. Available from http://www.nautilus.org/fora/Special-Policy-Forum/47_Albright.html; Internet; Accessed 13 February 2003.

Anderson, Sean K., and Stephen Sloan. *Historical Dictionary of Terrorism.* Lanham, MD:

"Attack on the USS Cole." Yemen Gateway. Available from http://www.al-bab.com/yeman/cole1.htm; Internet; Accessed 6 April 2004.

"2002 Bali Terrorist Bombing." *Wikipedia*, 2004 ed., s.v. Available from http://en.wikipedia.org/w/wiki.phtml?title=2002_Bali_terrorist_bombing&printable=yes; Internet; Accessed 17 March 2004.

Bowman, Steve. *Homeland Security: The Department of Defense's Role.* Congressional Research Service Report for Congress, Order Code RL 31615, 7, 14 May 2003.

_____. *Weapons of Mass Destruction: The Terrorist Threat.* Washington, D.C.: Congressional Research Service Report for Congress, 7 March, 2002. Available from http://www.fas.org/irp/crs/RL31332.pdf; Internet; Accessed 23 December 2002.

"'Chemistry 101': The Make-up and Importance of Radioisotopes." *Introduction to Radiological Terrorism*, 1. Available from http://www.nti.org/h_learnmore/radtutorial/chapter01_03.html; Internet; Accessed 19 May 2004.

CJCS CONPLAN 0500-98. *Military Assistance to Domestic Consequence Management Operations in Response to a Chemical, Biological, Radiological, Nuclear, or High-Yield Explosive Situation.* 11 February 2002.

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

Clark, C.J. *Mine/UXO Assessment: Former Yugoslav Republic of Macedonia.* New

Congressional Research Service. *Homeland Security: The Department of Defense's Role* RL 31615.

Crenshaw, Martha. "The Logic of Terrorism: Terrorist Behavior as a Product of Strategic Choice." In *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, rev. ed., edited by Walter Reich. Washington: Woodrow Wilson Center Press, 1998.

Defense Threat Reduction Agency. *Domestic WMD Incident Management Legal Deskbook*, 3-12 and 3-13, December 2003. Available at http://biotech.law.lsu.edu/blaw/DOD/manual; Internet; Accessed 23 April 2004.

Director of Central Intelligence, DCI Weapons Intelligence, Nonproliferation, and Arms Control Center. *Unclassified Report to Congress on the Acquisition of Technology Reacting to Weapons of Mass Destruction and Advanced Conventional Munitions, 1 January Through 30 June 2003*, 11. Available from http://www.cia.gov/cia/reports/721_reports/pdfs/jan_jun2003.pdf; Internet; Accessed 19 may 2004.

"Dirty Bombs: Response to a Threat." FAS Public Interest Report, *The Journal of the Federation of American Scientists* 55 no. 2 (March/April 2002), 1-11. Available from http://ww.fas.org/faspir/2002/v55n2/dirtybomb.htm; Internet; Accessed 15 April 2004.

DOD Directive 3025.1, *Military Support to Civil Authorities* (MSCA), 15 January 1993.

DOD Directive 3025.12, *Military Assistance for Civil Disturbances* (MACDIS), 4 February 1994.

DOD Directive 3025.15, *Military Assistance to Civil Authorities*, 18 February 1997.

"Fact Sheet on the Accident at the Chernobyl Nuclear Power Plant." U.S. Nuclear Regulatory Commission, 1. Available at http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/fschernobyl.html; Internet; Accessed 1 July 2004.

"Fact Sheet on the Accident at Three Mile Island." U.S. Nuclear Regulatory Commission, 1 to 5. Available at http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle,html; Internet; Accessed 1 July 2004.

Franks, Tommy. "General Tommy Franks Testimony on USS Cole." Washington, D.C., 25 October 2000. Available from http://www.fas.org/man/dod-101/sys/ship/docs/man-sh-ddg51-001025zd.htm; Internet; Accessed 5 April 2004.

"French Tanker Explosion Confirmed as Terror Attack." Available from http://www.ict.org.il/spotlight/det.cfm?id=837; Internet; Accessed 21 January 2004.

Harmon, Christopher C. *Terrorism Today*. London: Frank Cass Publishers, 2000;Reprint, Portland: Frank Cass Publishers, 2001.

"History of Radiological Terrorism." *Introduction to Radiological Terrorism, 1 to* 3. Available from http://www.nti.org/h_learnmore/radtutorial/chapter03_01.html; Internet; Accessed 19 May 2004.

"History of the United Nations and Chernobyl." The United Nations and Chernobyl, 1. Available at http://www.un.org/ha/Chernobyl; Internet; Accessed 1 July 2004

Hoffman, Bruce. "All You Need Is Love: How the Terrorists Stopped Terrorism." *Atlantic Monthly* December 2001: 1-6. Available from http://www.theatlantic.com/issues/_2001/12/hoffman.htm; Internet; Accessed 21 October 2002.

Joint Chiefs of Staff, *National Military Strategy of the United States of America*, 1, May 2004.

Joint Pub 1-02. *Department of Defense Dictionary of Military and Associated Terms*. 12 April 2001, as amended through 9 June 2004.

Joint Pub 3-07.2. *Joint Tactics, Techniques, and Procedures for Antiterrroism.* 17 March 1998.

Joint Task Force – Civil Support (JTF-CS)[U.S. Northern Command] website. Available at http://www.jtfcs.northcom.mil; Internet; Accessed 14 April 2004.

"Jordan 'was chemical bomb target'." BBC News UK Edition, 17 April 2004. Available at http://news.bbc.co.uk/1/hi/world/middle_east/3635381.stm; Internet; Accessed 28 April 2004.

Laqueur, Walter. *The New Terrorism: Fanaticism and the Arms of Mass Destruction.* Oxford: Oxford University Press, 1999.

Michel, Lou and Dan Herbeck. *American Terrorist: Timothy McVeigh and the Oklahoma City Bombing.* New York: Harper Collins Publishers Inc., 2001.

Moilanen, Jon H. "Engagement and Disarmament: A U.S. National Security Strategy for Biological Weapons of Mass Destruction." *Essays on Strategy XIII*. Washington, D.C.; National Defense University, 1996, 141-182.

National Commission on Terrorist Attacks Upon the United States. Statement of Brian Jenkins to the Commission, March 31, 2003. Available from http://www.9-11commission.gov/hearings/hearing1/witness_jenkins.htm; Internet; Accessed 23 September 2004.

Powell, William. *The Anarchist Cookbook*. Secaucus, NJ: Lyle Stuart, Inc., 1971.

"Terrorists and Radiological Terrorism." *Introduction to Radiological Terrorism*, 2 and 3. Available from http://www.nti.org/h_learnmore/radtutorial/chapter04_02.html; Internet; Accessed 19 May 2004.

"The Asymmetric Threat From Maritime Terrorism." Available from http://jfs.janes.com/public/jfs/additional_info.shtml; Internet; Accessed 2 February 2004.

The *Posse Comitatus Act*, 18 U.S.C. 1385

The *Robert. T. Stafford Disaster Relief and Emergency Assistance Act*, 42 U.S.C. 5121-5206

The White House. National Security Presidential Directive 17 (NSPD-17), *National Strategy to Combat Weapons of Mass Destruction*, 2, December 2002. Available at http://www.fas.org/irp/offdocs/nspd/nspd-17.html; Internet; Accessed 8 December 2003.

The White House, *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*. Washington, D.C., February 2003. Preface by The President of the United States of America. Available from http://www.whitehouse.gov/pcipb/physical_strategy.pdf; Internet; Accessed 8 December 2003.

The White House. *The National Security Strategy of the United Sates of America*, 1, 17 September 2002. Available at http://www.whitehouse.gov/nsc/nss.html; Internet; Accessed 30 April 2004.

U.S. Army Field Manual, FM 1, *The Army*, Washington, D.C., Headquarters, Department of the Army, 14 June 2005.

U.S. Army War College, *How The Army Runs; A Senior Leader Reference Handbook 2003-2004*. Carlisle, PA: U.S. Army War College, Department of Command, Leadership, and Management, 23 September 2003. Available at http://carlisle-www.army.mil/usawc/dclm/linkedtextchapters.htm; Internet; Accessed 31 December 2003.

U.S. Department of Defense. *Report to Congress on the Role of the Department of Defense in Supporting Homeland Security*...

U.S. Department of Defense. Washington Headquarters Services. Directorate for Information Operations and Reports. *Global War on Terrorism – Casualty Summary Operation Enduring Freedom*. Washington, D.C., As of 4 March 2004. Available from http://web1.whs.osd.mil/mmid/casualty/WOTSUM.pdf; Internet; Accessed 15 March 2004.

U.S. Department of Defense. Washington Headquarters Services. Directorate for Information Operations and Reports. *Table 13, Worldwide U.S. Active Duty Military Deaths, Selected Military Operations*. Washington, D.C., n.d. Available from http://web1.whs.osd.mil/mmid/casualty/table13.htm; Internet; Accessed 15 March 2004.

U.S. Department of Defense. Washington Headquarters Services. Directorate for Information Operations and Reports. *U.S. Active Duty Military Deaths – 1980 through 2002*. Washington, D.C., As of 10

April 2003. Available from http://web1.whs.osd.mil/mmid/casualty/Death_Rates.pdf; Internet; Accessed 16 January 2004.

U.S. Department of Defense. Washington Headquarters Services. Directorate for Information Operations and Reports. *War on Terrorism – Operation Iraqi Freedom, By Casualty Category within Type.* Washington, D.C., As of 26 February 2004. Available from http://web1.whs.osd.mil/mmid/casualty/OIF-Total.pdf; Internet; Accessed 15 March 2004.

U.S. Department of Homeland Security. *National Response Plan.* Washington, D.C.: U.S. Department of Homeland Security, November, 2004.

U.S. Department of State. Office of the Coordinator for Counterterrorism. *Patterns of Global Terrorism 2004.* Washington, D.C., 2004, revised 22 June 2004.

USNORTHCOM [U.S. Northern Command] website. Available at http://www.northcom.mil; Internet; Accessed 28 April 2004.

"What is Radiological Terrorism?" *Introduction to Radiological Terrorism*, 1 and 2. Available from http://www.nti.org/h_learnmore/radtutorial/chapter01_03.html; Internet; Accessed 19 May 2004.

This Page Intentionally Blank

"The battle is now joined on many fronts.
We will not waiver, we will not tire,
we will not falter, and we will not fail.
Peace and freedom will prevail…
To all the men and women in our military,
every sailor, every soldier, every airman,
every coast guardsman, every marine,
I say this: Your mission is defined.
The objectives are clear. Your goal is just.
You have my full confidence, and you will have
every tool you need to carry out your duty."

George W. Bush
The President of the
United States of America

Supplemental Handbook No. 1.04 ***Defense Support of Civil Authorities***
to DCSINT Handbook No.1 ***A Military Guide to Terrorism in the Twenty-First Century,*** **Version 3.0**
U.S. Army Training and Doctrine Command, Deputy Chief of Staff for Intelligence
Assistant Deputy Chief of Staff for Intelligence-Threats, Fort Leavenworth, Kansas