Joint Publication 3-07.2

Antiterrorism

14 April 2006

PREFACE

1. Scope

This publication provides doctrine on how to organize, plan, train for, and conduct joint antiterrorism operations.

2. Purpose

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

3. Application

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

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

For the Chairman of the Joint Chiefs of Staff:

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

Intentionally Blank

SUMMARY OF CHANGES
REVISION OF JOINT PUBLICATION 3-07.2
DATED 17 MARCH 1998

- **Provides a description of the overall operational context.**
- **Expands the discussion of protection, force protection, and antiterrorism relationships.**
- **Covers Department of Defense policy for the antiterrorism program.**
- **Discusses the role of the Assistant Secretary of Defense for Homeland Defense.**
- **Covers the Department of Defense's roles in homeland defense and support to civil authorities.**
- **Updates the discussion of terrorist threats to include the general shift in tactics and methodologies among international terrorists to produce mass casualties.**
- **Provides examples of terrorist asymmetric tactics, techniques, and procedures.**
- **Adds extensive coverage of countersurveillance.**
- **Adds a discussion of limits of military support to civil authorities.**
- **Annunciates the "No Double Standard" policy.**
- **Revises the antiterrorism program elements to include risk management, planning, training and exercises, resource generation, and program reviews.**
- **Defines risk management as having four subelements: criticality assessment, threat assessment, vulnerability assessment, and risk assessment.**
- **Greatly expands the concept of antiterrorism measures.**
- **Adds a discussion of design based threat.**
- **Covers barrier planning.**
- **Discusses range-to-effect charts and window upgrades.**

- **Covers suicide bombers/high risk vehicle checkpoints.**
- **Adds community engagement to the antiterrorism program.**
- **Completely revises coverage of incident response and consequence management.**
- **Adds considerations for incident response in the United States.**
- **Adds appendices on criticality assessment, threat assessment, and risk assessment.**
- **Adds appendices with sample antiterrorism plan format, antiterrorism checklist, and sample barrier plan.**
- **Adds appendix on the force protection condition system.**
- **Adds appendices on threat information organization matrix, homeland security advisory system, chemical, biological, radiological, and nuclear defense planning considerations, and joint antiterrorism program manager's guide.**
- **Redefines the terms "antiterrorism," "force protection," "force protection conditions," "terrorist," "terrorist group," and "terrorist threat level."**
- **Provides definitions for the terms "chemical, biological, radiological, and nuclear defense," "chemical, biological, radiological, nuclear, and high-yield explosive hazards," "criticality assessment," and "design basis threat."**

TABLE OF CONTENTS

Table of Contents

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Provides an Introduction to Antiterrorism**
- **Covers the Terrorist Threat**
- **Discusses Intelligence, Counterintelligence, Threat Analysis, and Countersurveillance**
- **Covers Legal Considerations**
- **Describes the Antiterrorism Program**
- **Discusses Preventative Measures and Considerations**
- **Covers Incident Response and Consequence Management**

Introduction

Combating terrorism

Combating terrorism involves actions including antiterrorism (AT) (defensive measures used to reduce the vulnerability to terrorist acts), counterterrorism (offensive measures taken to prevent, deter, preempt and respond to terrorism), consequence management (CM) (preparation for and response to consequences of a terrorist incident), and intelligence support (collection or dissemination of terrorism related information), taken to oppose terrorism throughout the entire threat spectrum.

Force protection (FP) should not be used as a synonymous term with antiterrorism (AT) or other supporting tasks.

Force protection (FP) is an overarching concept and mission responsibility inherent to command within all military operations. As discussed throughout this publication, AT, in contrast, is a sub-element of combating terrorism.

FP is a joint task.

Joint force commanders conduct FP in similar fashion to movement and maneuver; intelligence, surveillance, and reconnaissance; employing firepower; sustaining operations; operating in a chemical, biological, radiological or nuclear environment; and providing command and control during the execution of campaigns, major operations, and tactical engagements. FP actions are to be accomplished by the Services and by joint forces under joint command and control using joint doctrine. FP can be applied at multiple levels of command, from the strategic-theater, through the operational, and to the tactical level.

The Department of Defense's (DOD's) AT program is one of several programs that fall under the overarching FP concept.

The AT program is a collective, proactive effort focused on the detection and prevention of terrorist attacks against Department of Defense (DOD) personnel, their families, facilities, installations, and infrastructure critical to mission accomplishment as well as the preparations to defend against and planning for the response to the consequences of terrorist incidents. The minimum elements of an AT program are: risk management; planning; training and exercises; resource generation; and comprehensive program review.

Terrorist Tactics

The general shift in tactics and methodologies among international terrorists focuses on producing mass casualties.

Terrorists continue to adapt to conditions and develop more aggressive and effective methods, often incorporating multiple simultaneous attacks and suicide bombings. Their targets may be just as likely economic (tourists, financial networks) or agricultural ones (livestock, crops) as embassies or military forces/facilities. Their goal is not just to win favor for their causes, but to wage undeclared, unconventional war at will. The more common tactics employed by terrorist groups are assassination, arson, bombing, hostage taking, kidnapping, hijacking or skyjacking, seizure, raids or attacks on facilities, sabotage, hoaxes, use of weapons of mass destruction, and environmental destruction.

Threat Analysis

Terrorism threat analysis is a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups that could target the DOD components, elements, and personnel.

A threat analysis shall review the factors of a terrorist group's operational capability, intentions, and activity as well as the operating environment within which friendly forces operate. Threat analysis is an essential step in identifying and describing the threat posed by specific terrorist group(s) and/or individuals in a terrorism threat assessment. A vulnerability assessment is an evaluation to determine the vulnerability to a terrorist attack against an installation, unit, exercise, port, ship, residence, facility, or other site. In accomplishing this assessment, it is important to consider the design basis threat to determine the facility's design and structural requirements. The threat assessment and vulnerability assessment are then utilized with the criticality assessment to provide the basis for risk management decisions. Commanders must determine which assets require the most protection and where future expenditures are required to minimize risk of attack or lessen the severity of the outcome of an attack.

Intelligence and Counterintelligence

Intelligence and counterintelligence are critical in the development of an AT program.

Strategic, well-planned, proactive, systematic, all-source intelligence and counterintelligence (CI) programs are essential. The role of intelligence and CI is to identify, assess, deter, disrupt, and defeat the threat, provide advance warning, and disseminate critical information/intelligence in a usable form for the commander. All command personnel may potentially contribute to information collection and analytical efforts. Effective intelligence and CI support requires effort to execute the intelligence process and to conduct effective operations and investigations against the threat. The entire process is important in providing decision makers with information and timely warnings upon which to recommend FP actions.

Community Engagement

Effective AT efforts extend beyond the peerimeter.

Commanders increase their capability to refine the local threat picture and shape their operating environment by appropriate coordination and interaction with local area residents. Whether inside the United States or at an expeditionary location, effective communication and developed rapport among area leaders, nongovernmental organizations, businesses, residents, and military leaders support the defense-in-depth concept and ensure the first layer of defense extends beyond the base perimeter. Local language and cultural training for appropriate personnel also contribute to rapport development.

Legal Considerations

Commander's authority.

A commander's responsibility and authority to enforce security measures and to protect persons and property are critical during any level of conflict. Commanders should consult with their legal advisors often when establishing their AT programs. Legal personnel should be members of all installation or unit AT cells, boards, and working groups.

Constraints and restraints on military support to civil authorities.

DOD is the lead, supported by other agencies, in defending against traditional external threats/aggression against the US homeland. However, against internal, asymmetric, or nontraditional threats (e.g., terrorism), DOD may be in support of the Department of Homeland Security or another lead or primary agency. When providing support to civil authorities, DOD will do so as directed by the President or the Secretary of Defense and consistent with laws, Presidential directives, executive orders, and DOD policies and directives. The following general principles apply to such support:

Except in the case of immediate response authority, DOD resources are provided only when response or recovery requirements are beyond the capabilities of local, state, and Federal civil authorities, and when they are requested by a lead or primary agency and approved by the Secretary of Defense.

In certain circumstances, **imminently serious conditions resulting from either civil emergencies or attacks may require immediate response by military commanders**. Responses to requests from civil authorities prior to receiving authority from the President or chain of command are made when immediate support is critical **to save lives, prevent human suffering, or mitigate great property damage**.

Antiterrorism Program

The AT program stresses deterrence of terrorist incidents through preventive measures common to all combatant commands and Services.

In order to be successful, an AT program must be implemented in a methodical, coordinated manner. It cannot be stressed enough that the AT program is the ultimate responsibility of the commander or, in the case of a DOD agency, the civilian equivalent, who has the authority and responsibility to alter or add to the AT program as deemed necessary to accommodate the local situation. The minimum AT program elements include risk management, planning, training and exercises, resource generation, and program reviews. Plans for CM and incident response are important adjuncts to an effective AT program.

Risk management is the process of systematically identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk costs with mission benefits. The commander must decide how best to employ given resources and AT measures to deter, mitigate, and prepare for a terrorist incident while continuing the mission. Risk management has four key subelements: criticality assessment; threat assessment; and vulnerability assessment.

The criticality assessment provides the commander with a prioritized list of assets based on the necessity for mission completion. The terrorism threat assessment is the tool that commanders use to determine the capability, intentions, and activity of terrorist organizations. The vulnerability assessment is the determination of susceptibility to attack by the broad range of terrorist threats. The risk assessment combines the criticality, threat, vulnerability, and risk assessments.

Preventive Measures and Considerations

Commander's responsibility to manage terrorism risk.

Although the risk of terrorist aggression against US and multinational resources cannot be totally eliminated, it can be reduced and managed through deliberate and effective risk management. Command planning and execution should include actions to implement AT measures which are consistent with fundamental risk management principles. Through the application of the basic risk management principles of identification, assessment, risk avoidance, loss prevention, loss reduction, and process evaluation/reapplication, most FP requirements can be met.

Preventive and protective security measures should be taken by military units and individual Service members to protect themselves and their ability to accomplish their mission during mobilization, deployment, employment, sustainment, and redeployment operations. Additionally, rest and recuperation (R&R) facilities and other facilities not located in a traditional military installation also require close consideration. These facilities are frequently vulnerable due to their location and generally easy access. Service personnel are at risk of lowering their guard while using these R&R facilities. The installation, ship, unit, or port AT plan provides the mechanism to ensure readiness against terrorist attacks while the unit performs its tactical mission during deployments.

Incident Response and Consequence Management

Incident management is a sequence of command, staff, and first responder actions to respond to a terrorist incident or other unique event and restore AT capability.

The primary objective of incident response management is to mitigate the effects and number of casualties resulting from a terrorist attack. Commanders develop response measures to save lives, preserve health and safety, secure and eliminate the hazard, protect property, prevent further damage to the installation, and maintain public confidence in the installation's ability to respond to a terrorist incident.

CM is the preparedness and response to mitigate the consequences of an incident resulting from the use of chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE) agents. It includes mass alerting or notification capabilities, disaster planning, public health, medical surveillance and other preparatory efforts.

A commander's responsibility and authority to enforce security measures and to protect persons and property is of utmost importance during any level of conflict. As such, it is incumbent upon the commander to plan for, and be capable of reacting to, a terrorist attack. Attacks employing CBRNE weapons may produce massive casualties or widespread destruction, which can quickly overwhelm organic resources.

CONCLUSION

This publication provides doctrine on how to organize, plan, train for, and conduct joint antiterrorism operations and interagency AT coordination.

CHAPTER I
INTRODUCTION

"There is another type of warfare — new in its intensity, ancient in its origin — war by guerrillas, subversives, insurgents, assassins; war by ambush instead of by combat, by infiltration instead of aggression, seeking victory by eroding and exhausting the enemy instead of engaging him . . . It preys on unrest . . . "

John F. Kennedy
Address to the Graduating Class,
US Naval Academy, 6 June 1962

1. General Operational Context

Antiterrorism (AT) is a defensive component of combating terrorism (CbT). Defensive elements of CbT are part of force protection (FP).

a. The terrorism threat: Although there is no universal definition for terrorism, the Department of Defense (DOD) defines it 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. Terrorists operating worldwide pose grave dangers to the Armed Forces of the United States, and the assurance that our forces can accomplish their missions.

b. Specific policy, directive guidance, standards, and procedures for the DOD AT program is contained in DOD Directive (DODD) 2000.12, *DOD Antiterrorism (AT) Program*, DOD Handbook O-2000.12-H, *DOD Antiterrorism Handbook,* and Department of Defense Instruction (DODI) 2000.16, *DOD Antiterrorism Standards*.

2. Purpose

a. CbT (see Figure I-1) involves actions including AT (defensive measures used to reduce the vulnerability to terrorist acts), counterterrorism (CT) (offensive measures taken to prevent, deter, preempt, and respond to terrorism), consequence management (CM) (preparation for and response to consequences of a terrorist incident), and intelligence support (collection or dissemination of terrorism-related information), taken to oppose terrorism throughout the entire threat spectrum. CbT is no longer just about apprehending and prosecuting terrorists, limiting damage, and managing consequences. The national strategy intends to stop terrorist attacks against the United States, its citizens, its interests, and our friends and allies around the world and ultimately, to create an international environment inhospitable to terrorists and all those who support them. In order to accomplish these tasks we simultaneously:

(1) Defeat terrorist organizations of global reach by attacking their sanctuaries; leadership; command, control, and communications; material support; and finances.

Figure I-1. Combating Terrorism

(2) Deny further sponsorship, support, and sanctuary to terrorists by ensuring other states accept their responsibilities to take action against these international threats within their sovereign territory.

(3) Diminish the underlying conditions that terrorist seek to exploit by enlisting the international community to focus its efforts and resources on the areas most at risk.

(4) Defend the United States, our citizens, and our interests at home and abroad by both proactively protecting our homeland and extending our defenses to ensure we identify and neutralize the threat as early as possible. AT is a key contributor to this effort..

b. This publication does not address CT. The following definitions, also shown in Figure I-2, are provided to assist in understanding the difference between AT and CT:

(1) Antiterrorism is defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces.

(2) Counterterrorism is the offensive measures taken to prevent, deter, preempt, and respond to terrorism. Sensitive and compartmented CT programs are addressed in relevant national security decision directives, national security directives, joint operation plans (OPLANs), and other relevant classified documents.

3. Protection, Force Protection, and Antiterrorism Relationships

a. Actions to protect the force must be developed during all phases in order to support the joint force commander (JFC) concepts of operations. FP remains a command responsibility. As discussed throughout this publication, AT, in contrast, is a sub-element of CbT, which is a subset

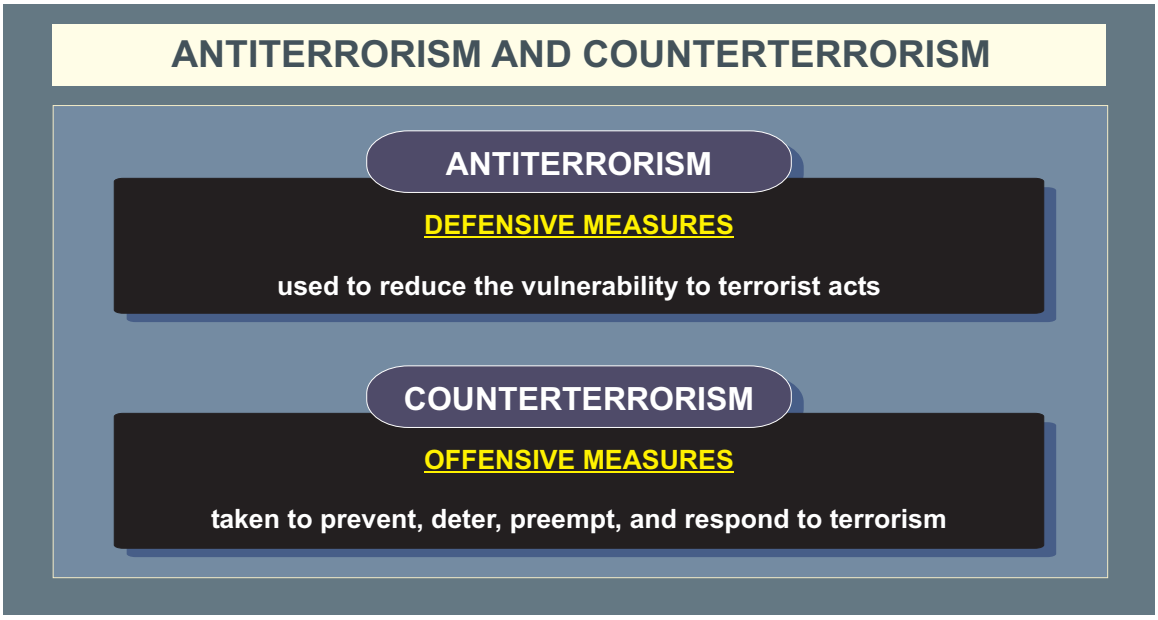


Figure I-2. Antiterrorism and Counterterrorism

of the broader FP concept. FP is one line of effort in the overall effort to achieve protection. FP and other supporting elements' relationships are depicted in Figure I-3. Protection is the end state. Core efforts protect different elements necessary for protection, including people, assets, processes, information, and interdependent networks and systems. The elements listed in the vertical columns are representative of programs and endeavors that support all three lines of effort. For instance, physical security measures contribute directly to FP, continuity of operations (COOP), and critical infrastructure protection. Similarly, CbT, and its AT component, support all three core efforts as well. These supporting programs rely on effective policy, interagency cooperation, technology, legal support, and appropriate resources. Implementation of all efforts is based on the corresponding commanders' risk management processes.

(1) The protection function focuses on conserving the joint force's fighting potential in three primary ways: active offensive and defensive measures (such as air defense) that protect the joint force, its information, its bases, necessary infrastructure, and lines of communications (LOCs) from an adversary's attack; passive measures (such as concealment) that make friendly forces, systems, and facilities difficult to locate, strike, and destroy; and applying technology and procedures to reduce the risk of fratricide. As the JFC's mission requires, the protection function also extends beyond force protection to encompass protection of US noncombatants; the forces, systems, and civil infrastructure of friendly nations; and other government agencies , intergovernmental organizations (IGOs), and nongovernmental organizations (NGOs). Protection capabilities apply domestically in the context of homeland defense (HD) and civil support. The protection function encompasses a number of tasks, including:

(a) Collecting information for indications and warning.

(b) Providing air, space, and missile defense.

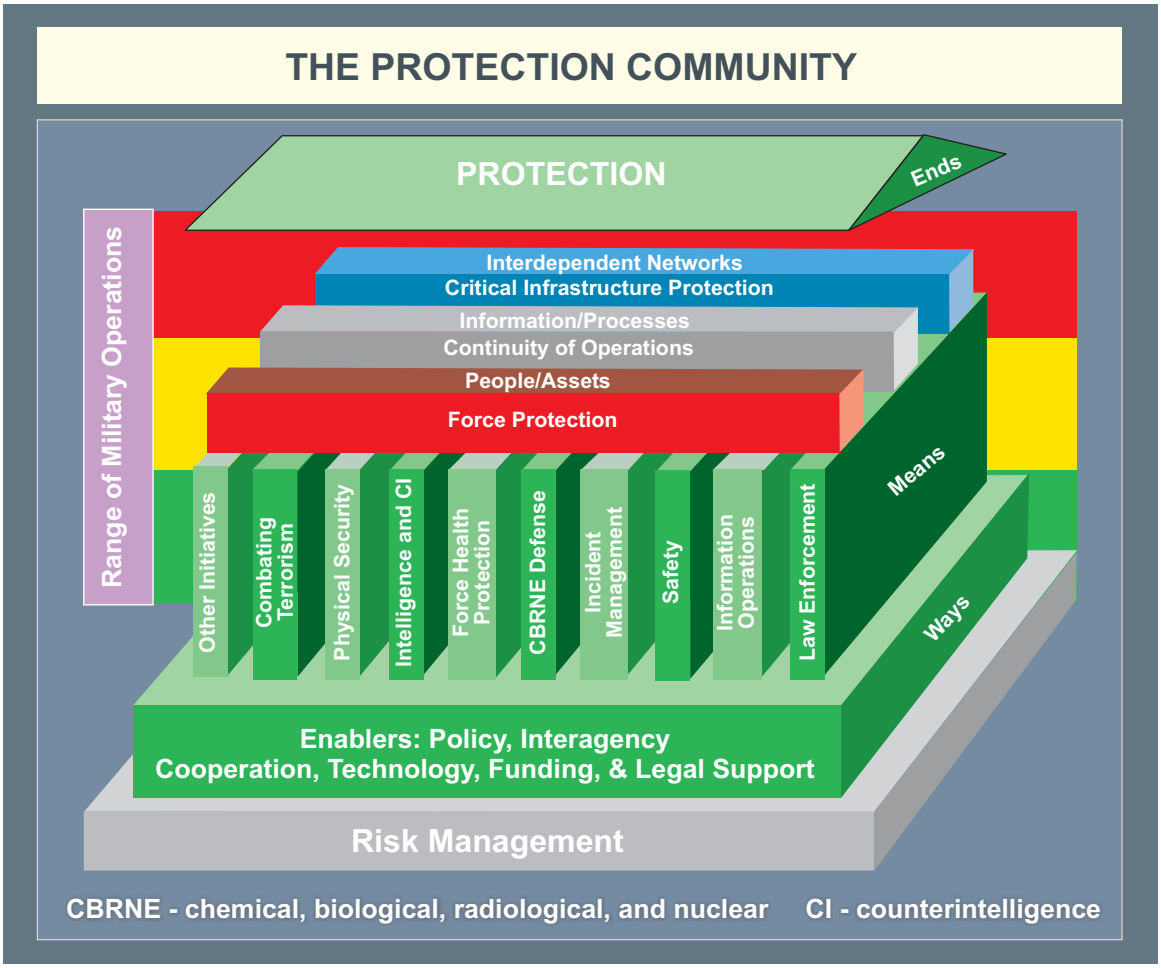


Figure I-3. The Protection Community

(c) Protecting noncombatants, including conducting noncombatant evacuation operations when required. See subparagraph 2b of Chapter VI, "Crisis Response Contingency Operations."

(d) Providing physical security for forces and means.

(e) Conducting defensive countermeasure operations, including counter-deception and counterpropaganda operations.

(f) Providing nuclear, biological, and chemical defense.

(g) Conducting information operations (IO) in defensive operations (including operations security [OPSEC]).

(h) Securing and protecting flanks, rear areas, and LOCs.

(i) Conducting chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE) CM.

(j) Conducting antiterrorism operations.

(k) Providing health services.

(l) Establishing capabilities and measures to enhance safety and prevent fratricide.

(2) **FP.** Actions taken to prevent or mitigate hostile actions against DOD personnel (to include family members), resources, facilities, and crucial information. FP does not include actions to defeat the enemy or protect against accidents, weather, or disease. FP is a joint task. As such, JFCs conduct FP in similar fashion as movement and maneuver; intelligence, surveillance, and reconnaissance (ISR); employing firepower; sustaining operations; operating in a CBRNE environment; and providing command and control (C2) during the execution of campaigns, major operations, and tactical engagements. FP actions are a command responsibility at all levels of command.

(3) **AT.** AT is defined as: "Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces." While AT integrates other defensive actions (such as physical security, chemical, biological, radiological, and nuclear (CBRN) defense, operations security, counterintelligence (CI), construction standards, etc.) in a comprehensive program designed to protect against terrorist attack, it does not include all the aspects of FP.

b. In order to prevent or mitigate redundant or parallel programs, plans, and capabilities developed for AT should be applied as necessary to other crisis or incident management efforts.

4. Overview of Antiterrorism Program Elements

The DOD's AT program is one of several programs that fall under the FP concept. The AT program is a collective, proactive effort focused on the detection and prevention of terrorist attacks against DOD personnel, their families, facilities, installations, and infrastructure critical to mission accomplishment as well as the preparations to defend against and planning for the response to the consequences of terrorist incidents. Although not elements of AT, plans for terrorism CM preparedness and incident response measures as well as plans for continuing essential military operations are important adjuncts to an effective AT program. The minimum elements of an AT program are: risk management; planning; training and exercises; resource generation; and comprehensive program review. **Risk** is the probability and severity of loss linked to hazards. **Risk management** is the process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk cost with mission benefits. The process, or sequence, of AT program elements should be iterative and serve continuously to refine the AT plan.

Every commander has the responsibility for the security of the command against terrorist attacks.

5. Overview of Department of Defense Role and Responsibility

a. **DOD policy**

(1) The DOD components, elements, and personnel shall be protected from terrorist acts through a high priority, comprehensive AT program. The DOD's AT program shall be all encompassing using an integrated systems approach.

(2) Commanders at all levels have the responsibility and authority to enforce appropriate security measures to ensure the protection of DOD elements and personnel (including deployed DOD contractors accompanying the Armed Forces of the United States, if warranted under DODI 3020.41, *Contractor Personnel Authorized to Accompany the US Armed Forces*) subject to their control. Commanders should ensure the AT awareness and readiness of all DOD elements and personnel (including dependent family members) assigned or attached. Commanders must also ensure appropriate AT protection and readiness of DOD elements and personnel (including deployed DOD contractors accompanying the Armed Forces of the United states, if warranted under DODI 3020.41, *Contractor Personnel Authorized to Accompany the US Armed Forces*) while pursuing mission accomplishment.

(3) The geographic combatant commanders' AT policies take precedence over all AT policies or programs of any DOD component operating or existing in that command's area of responsibility (AOR) except for those under the security responsibility of a chief of mission (COM). Contingency contractor personnel who accompany US military forces shall complete pre-deployment processing specified in DODI 3020.41, *Contractor Personnel Authorized to*

Accompany the US Armed Forces, including antiterrorism training. All DOD personnel traveling into or through a combatant commander's AOR will familiarize themselves with all AOR-specific AT policies and comply with them.

(4) A Combating Terrorism Readiness Initiatives Fund (CbT-RIF) is maintained to provide a flexible means to respond to emergent and/or emergency AT requirements (Chairman of the Joint Chiefs of Staff Instruction [CJCSI] 5261.01D, *Combating Terrorism Readiness Initiatives Fund*). More information can be found online at "https://www.atep.smil.mil."

(5) All personnel on DOD-related travel shall comply with theater, country, and special clearance requirements (DODD 4500.54, *Official Temporary Duty Travel Abroad*, and DODD 4500.54-G, *DOD Foreign Clearance Guide (FCG)*), before overseas travel. Contractors deploying with or otherwise providing support in a theater of operations to the Armed Forces of the United States deployed outside the US conducting contingency operations or other military operations, shall comply with DODI 3020.41, *Contractor Personnel Authorized to Accompany the US Armed Forces*.

(6) Commanders shall develop a security plan for contingency contractor personnel in locations where the geographic combatant commander decides there is not sufficient or legitimate civil authority and the commander decides that it is in the interest of the government to provide security because the contractor cannot obtain effective security services, such services are unavailable at a reasonable cost, or threat conditions necessitate security through military means. The contracting officer shall include in the contract the level of protection to be provided to contingency contractor personnel. In appropriate cases, the geographic combatant commander may provide security through military means, commensurate with the level of security provided DOD civilians. Specific security measures shall be mission and situation dependent as determined by the geographic combatant commander. DOD shall assist the Department of State (DOS), where militarily feasible, in supporting efforts to protect US citizens abroad. Contractors may be required, based upon terms of their contract, to contact the combatant command or designated subordinate command to obtain, and comply with, the specific AT guidance for that particular area. Similarly, commanders may be required to offer AT training to contractors. Contractors, working within a US military facility or in close proximity of US forces, shall receive, incidentally, the benefits of measures undertaken to protect US forces. Additionally, commanders may provide an additional, higher level of security, to which the government may have agreed pursuant to a particular contract.

(7) Compliance with the "No Double Standard" policy on dissemination of terrorist threat information is maintained. (See Chapter IV, "Legal Considerations.")

b. **DOD Responsibilites**

(1) **Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict) (ASD[SO/LIC])**

(a) Serve as Antiterrorism Coordinating Committee-Senior Steering Group (ATCC-SSG) Co-Chair.

(b Monitor programs to reduce the vulnerability of DOD personnel and their family members, facilities, and other DOD materiel to terrorist attack with the Chairman of the Joint Chiefs of Staff (CJCS) and other DOD components.

(c) Ensure compliance with DODD 2000.12, *DOD Antiterrorism (AT) Program*.

(d) Oversee High-Risk Personnel (HRP) Program.

(2) **Assistant Secretary of Defense (Homeland Defense) (ASD[HD]).** The principal duty of the ASD(HD) is to provide overall supervision of HD and civil support activities within DOD. In that role, the ASD(HD) responsibilities include:

(a) Developing strategic planning guidance for DOD's role in homeland security (HS).

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

(c) Overseeing DOD activities that provide defense support of civil authorities in domestic emergencies in accordance with existing national level emergency response plans and approved memoranda of understanding (MOUs).

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

(e) Serving as the DOD domestic crisis manager focusing on coordination and integration of DOD domestic crisis activities with other departments and agencies and the combatant commanders. Exceptions include those activities requiring the use of special operations forces.

(f) Assuming responsibility for the Defense Critical Infrastructure Program (DCIP), HD interagency coordination, HD technology transfer, national security special events, and COOP.

(3) **The Secretaries of the Military Departments shall**

(a) Institute and support AT programs in accordance with DODD 2000.12, *DOD Antiterrorism (AT) Program*.

(b) Provide AT resident training to personnel assigned to high-risk billets (HRBs) and others as appropriate.

(c) Ensure military construction programming policies include AT protective features for facilities and installations.

(d) Provide a representative as a member of the DOD Antiterrorism Coordinating Committee (ATCC) and subcommittees, as required.

(e) Ensure all assigned military, DOD civilians, DOD contractors, and their family members receive applicable AT training and briefings pursuant to DODI 2000.16, *DOD Antiterrorism Standards*. Ensure personnel traveling to a geographic combatant commander's AOR comply with DODD 4500.54, *Official Temporary Duty Travel Abroad*, and DODD 4500.54-G, *DOD Foreign Clearance Guide (FCG)*. Ensure personnel are aware of any DOS travel warnings in effect at the time of travel.

(4) **The Chairman of the Joint Chiefs of Staff shall**

(a) Serve as the principal advisor to the Secretary of Defense (SecDef) for all DOD AT issues.

(b) Prepare joint doctrine and assist the ASD(SO/LIC) in development and maintenance of the AT program, standards and procedures. Review doctrine, policy, standards, and procedures of the DOD components. Review, coordinate, and oversee for the SecDef and in conjunction with the DOD components and Services, the AT training for all DOD personnel (including their dependent family members).

(c) Ensure the Chairman's Program Review and the Chairman's Program Assessment include a summary of AT requirements as determined by the Joint Requirements Oversight Council and derived from combatant commander integrated priority lists.

(d) Assist ASD(SO/LIC) with centralized policy and standard development for HRP programs, training, and support.

(e) Annually, as part of the DOD Planning, Programming, Budgeting, and Execution (PPBE) cycle, assist the Military Departments in determining the merit of AT requirement submissions. Review the adequacy of resources proposed by the Military Departments to determine whether they meet AT objectives and support combatant commanders' AT programs. Coordinate and make recommendations on unresolved AT requirements during programming and budget reviews. These reviews shall be done in conjunction with the Office of the Secretary of Defense (OSD) principal staff assistants having resource, program, and budget oversight responsibilities for the functional areas that comprise the AT budget aggregate. Advise the SecDef of any changes needed to meet AT requirements.

(f) Assess the DOD components' AT policies and programs for the protection of DOD elements and personnel, including DOD-owned, leased, or managed infrastructure and assets critical to mission accomplishment and other DOD-owned, leased or managed mission essential assets. Ensure assessments are conducted of CJCS exercises, air/sea ports of embarkation/debarkation, and in-transit forces.

(g) Assess AT as an element of the overall force planning function of any force deployment decision. Periodically reassess AT posture of deployed forces. Review combatant commanders' joint OPLANs, operation plans in concept format, and functional plans, deployment orders, and other relevant documents for AT issues.

(h) Assess the implementation of force protection conditions (FPCONs) for uniform implementation and dissemination as specified by DODD 2000.12, *DOD Antiterrorism (AT) Program*, DODI 2000.16, *DOD Antiterrorism Standards*, and DOD Handbook O-2000.12-H, *DOD Antiterrorism Handbook*.

(i) Provide representatives to the DOD ATCC and appropriate subcommittees as required under enclosure 3 of DODD 2000.12, *DOD Antiterrorism (AT) Program*. Provide an observer to the Overseas Security Policy Board. Appoint the Director for Operations, Joint Staff (J-3) to co-chair the ATCC-SSG and the J-3 Deputy Director for Antiterrorism and Homeland Defense to co-chair the ATCC under enclosure 3 of DODD 2000.12, *DOD Antiterrorism (AT) Program*.

(j) Coordinate with the Under Secretary of Defense for Intelligence and the ASD(SO/LIC) on sharing of terrorism intelligence and CI data and law enforcement (LE), suspicious activity report (SAR) information on AT. This includes threats posed to DOD components, elements, and personnel by domestic and foreign terrorists.

(k) Assess the capability of the Military Departments, the combatant commands, and the DOD intelligence and security organizations to collect, receive, evaluate, analyze, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack. Also assess the capability to fuse SARs from military security, LE, and CI organizations with national-level ISR collection activities.

(l) In coordination with the ASD(SO/LIC), manage and administer the CJCS CbT-RIF pursuant to CJCSI 5261.01D, *Combating Terrorism Readiness Initiatives Fund*. Ensure out-year maintenance costs for CbT-RIF-funded projects are identified and coordinated with the Military Departments so that they are addressed during the PPBE cycle.

(m) Maintain a centralized database of all vulnerability assessments (VAs) conducted. Prepare and disseminate analysis of DOD-wide AT vulnerability trends correlated to Military Department efforts within the process.

(n) Be responsible for policy guidance and oversight of the Antiterrorism Enterprise Portal (ATEP).

1. ATEP encompasses the policies, procedures, and information systems that support trained personnel in managing the elements of an AT program, from the Joint Staff through the operating forces and components, across the range of military operations. These elements include risk management; planning, training and exercises; resource generation; and comprehensive program review.

2. The ATEP system is a comprehensive web enabled system that provides the Joint Staff, combatant commands, Services, DOD agencies, DOD field activities, subordinate task forces and components, and others with information processing and dissemination capabilities necessary for AT programs.

(o) Review planned and on-going information operations and community engagement programs for AT content and effectiveness.

(5) **Geographic combatant commanders shall**

(a) Establish AT programs and procedures for the protection of all DOD elements and personnel in their AOR, including those for whom the combatant commander assumes AT responsibility based on a memorandum of agreement (MOA) with a COM. Coordinate with the COMs in the AOR to identify all noncombatant commander DOD components and DOD elements and personnel. In instances where AT protection may be more effectively provided through the combatant commander, establish country-specific MOAs.

(b) Ensure AT programs and procedures include specific prescriptive standards derived from DODI 2000.16, *DOD Antiterrorism Standards*, to address specific terrorist capabilities and geographic settings, particularly regarding infrastructure critical to mission accomplishment and other DOD-owned, leased, or managed mission essential assets.

(c) Establish FP programs and procedures for all DOD personnel in the combatant commander's AOR. Combatant commanders with geographic responsibilities shall exercise authority for FP over all DOD personnel (including their dependents) assigned, attached, transiting through, or training in the combatant commander's AOR; except for those for whom the COM retains security responsibility. This authority enables combatant commanders to change, modify, prescribe, and enforce FP measures for covered forces. Directives from combatant commanders having authority for FP should consider the worldwide mission of those commanders with global responsibilities. Transient forces do not come under the chain of command of the area commander solely by their movement across operational area boundaries, except when the combatant commander is exercising tactical control (TACON) authority for FP purposes.

(d) Ensure policies and procedures are in place to identify and designate incumbents of HRBs and dependent family members requiring AT resident training. Provide supplemental training, as required, to personnel assigned to HRBs or designated as high-risk persons.

(e) Periodically, assess and review the AT programs of all assigned and attached DOD components in their AOR. Assess the AT programs of all DOD components performing in their AOR that are not under the authority of a COM. Component commands may be delegated responsibility to conduct these assessments. Ensure AT program reviews include a validation of the risk management methodology used to assess asset criticality, terrorist threat, and vulnerabilities. AT program reviews shall also evaluate installation and activity preparedness to respond to terrorist incidents (including CBRNE incidents), and the plans for managing the

consequences of terrorist incidents and maintaining continuity of essential military operations. Relocate forces as necessary and report to the SecDef through the CJCS pertinent actions taken for protection.

(f) Consistent with DODI 5210.84, *Security of DOD Personnel at US Missions Abroad*, and all appropriate MOUs, serve as the DOD point of contact with host-nation (HN) officials on matters involving AT policies and programs.

(g) Provide updates to DODD 4500.54, *Official Temporary Duty Travel Abroad*, and DODD 4500.54-G, *DOD Foreign Clearance Guide (FCG)*, stating command travel requirements and theater entry requirements.

(h) Upon arrival in their AOR, ensure all assigned military, DOD civilians, and their family members received applicable AT training and briefings pursuant to DODI 2000.16, *DOD Antiterrorism Standards*. Ensure personnel traveling within or through their AOR comply with DODD 4500.54, *Official Temporary Duty Travel Abroad*, and DODD 4500.54-G, *DOD Foreign Clearance Guide (FCG)*. Ensure personnel are aware of any DOS travel warnings in effect at the time of travel. Provide information necessary to ensure that all DOD personnel (including dependent family members) scheduled for permanent change of station to their AOR may receive required AT training and briefings (e.g., AOR updates) in compliance with DODI 2000.16, *DOD Antiterrorism Standards*, before departing previous assignment. Identify and disseminate to deploying force providers specific AOR pre-deployment training requirements that all personnel, including contractors deploying with the force, must complete before arrival in theater. All contingency contractor personnel shall comply with applicable combatant commander and local commander force protection policies.

(i) Identify, document, validate, prioritize, and submit to the Joint Staff the resource requirements necessary to achieve the AT program objectives for each activity under the combatant commander or for which that commander has responsibility. Work with the Joint Staff and the Service component commands to ensure that resource requirements to implement the AT programs are identified and programmed according to PPBE procedures.

(j) Establish command relationships and policies for subordinate commands, including joint task forces (JTFs), to ensure that effective mechanisms are in place to maintain protective posture commensurate with the terrorist threat.

(k) Assess the terrorist threat for the AOR according to DODD 2000.12, *DOD Antiterrorism (AT) Program*, and provide threat assessment (TA) information to the DOD components and the COMs in the AOR. Develop risk mitigation measures and maintain a database of those measures and the issues that necessitated their implementation. On the basis of the TA, identify and designate incumbents of HRBs and dependent family members to receive AT resident training.

(l) Keep subordinate commanders informed of the nature and degree of the threat. Ensure that commanders are prepared to respond to changes in threats and local security circumstances. Ensure that the COMs are fully and currently informed of any threat information relating to the security of those DOD elements and personnel under their responsibility, but not under the command of the combatant commander.

(m) Ensure compliance with the "No-Double-Standard" policy (see Chapter IV, "Legal Considerations").

(n) Submit to the CJCS emergent and/or emergency AT requirements that cannot be funded by the Military Departments for CbT-RIF funding consideration.

(o) Ensure FPCONs are uniformly implemented and disseminated as specified by DODD 2000.12, *DOD Antiterrorism (AT) Program*, DODI 2000.16, *DOD Antiterrorism Standards*, and DOD O-2000.12-H, *DOD Antiterrorism Handbook*.

(p) Coordinate AT program issues with the functional combatant commanders, the COMs, the DOD agencies and field activities, and the Military Departments, as appropriate.

(q) Provide a representative to the DOD ATCC and appropriate subcommittees, as required under enclosure 3 of DODD 2000.12, *DOD Antiterrorism (AT) Program*.

(r) Ensure a capability exists to collect, receive, evaluate, analyze, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack. Develop and implement the capability to fuse suspicious activity reports from military security, LE, and CI organizations with national-level ISR collection activities.

(s) Develop an AOR, combatant commander-oriented AT strategic plan that details the vision, mission, goals, and performance measures in support of the DOD's AT Strategic Plan.

(6) **Functional combatant commanders shall**

(a) Establish AT policies and programs for assigned DOD elements and personnel including assessment and protection of facilities and appropriate level of AT training and briefings. Coordinate programs with the appropriate geographic combatant commander and COM.

(b) Coordinate with the geographic combatant commanders to ensure adequate AT protection of forces.

(c) Ensure that subordinate elements, which are tenant units on Military Service installations, coordinate their AT programs and requirements with the host installation commander. Differences shall be resolved through the applicable combatant commander and the Service component command chain of command.

(d) Identify and designate incumbents of HRBs and dependent family members requiring AT resident training. Provide AT resident training to personnel assigned to HRBs and others, as applicable. Identify designated HRPs annually to the Services and CJCS.

(e) For emergent and/or emergency AT requirements that cannot be funded through other means, submit requirements to the CJCS for CbT-RIF consideration.

(f) Provide a representative to the DOD ATCC and appropriate subcommittees, as required under enclosure 3 of DODD 2000.12, *DOD Antiterrorism (AT) Program*.

(g) Identify, document, and submit to the Joint Staff the resource requirements necessary to achieve AT program objectives for each activity under the combatant command or for which the commander has responsibility. Work with the Service component commands to ensure that resource requirements to implement the AT programs are identified and programmed according to PPBE procedures.

(h) Develop their own combatant commander-oriented AT strategic plan that details the vision, mission, goals, and performance measures in support of the DOD and geographic combatant commanders' AT strategic plans.

(7) **Directors of other DOD agencies and field activities, OSD, principal staff assistants, and those that report directly to the Secretary or Deputy Secretary of Defense, shall**

(a) Support the geographic combatant commanders as they exercise overall FP responsibility and execute their AT programs for the personnel and resources within their respective AOR. Institute AT programs, ensure that DOD agencies and field activities conduct vulnerability assessments that address terrorism as a potential threat to the DOD elements and personnel, and incorporate AT measures into contingency response plans.

(b) Utilize DOD O-2000.12-H, *DOD Antiterrorism Handbook*, and DODI 2000.16, *DOD Antiterrorism Standards*, for the AT planning and execution for their headquarters (HQ) and all activities under their cognizance: consider mission, characteristics of the activity, geographic location, threat level, and FPCON. Establish prescriptive AT standards for installations and facilities not located on US military installations. Coordinate with the applicable combatant commander to ensure AT polices and programs are in concert with the geographic combatant commanders' overall responsibility for the AOR.

(c) Comply with DODI 2000.16, *DOD Antiterrorism Standards*, requirements to maintain an AT training and exercise program. Ensure that all assigned personnel comply with DODD 4500.54, *Official Temporary Duty Travel Abroad,* and DODD 4500.54-G, *DOD Foreign Clearance Guide (FCG)*. Ensure that personnel are aware of any travel security advisories in effect at the time of travel. Ensure that all DOD personnel (including dependent family members) scheduled for permanent changes of station to foreign countries receive required AT training or briefing specified in DODI 2000.16.

(d) Provide members to the DOD ATCC and appropriate subcommittees, as required under enclosure 3 of DODD 2000.12, *DOD Antiterrorism (AT) Program*.

(e) As part of the PPBE cycle, identify and document resource requirements necessary to implement and maintain AT programs. Submit AT requirements to the SecDef with an information copy to the CJCS and the appropriate combatant commanders. Include resource requirements in program and budget submissions. For emergent and/or emergency AT requirements that cannot be funded through other means, submit requirements through the appropriate combatant commander to the CJCS for CbT-RIF consideration. Implement accounting procedures to enable precise reporting of data submitted to Congress in the Congressional Budget Justification Book, including the number and cost of personnel directly supporting the DOD's AT program.

(f) Identify and designate incumbents of billets that are potentially high-risk targets of terrorist attacks and dependent family members requiring AT resident training. Ensure that AT resident training is provided to personnel assigned to HRBs and others, as applicable.

(g) Ensure that current physical security technology and security requirements are incorporated into all new contracts, where appropriate.

(h) Ensure AT protective features for facilities and installations are included in the planning, design, and execution of military and minor construction projects to mitigate vulnerabilities and terrorist threats (Unified Facilities Criteria [UFC] 4-010-01, *DOD Minimum Antiterrorism Standards for Buildings*, UFC 4-010-02, *DOD Minimum Antiterrorism Standoff Distances for Buildings*, and UFC 4-021-01, *Design and O&M: Mass Notification Systems*).

(i) Develop an AT strategic plan that details the vision, mission, goals, and performance measures in support of the DOD's AT Strategic Plan.

c. With respect to CbT and other homeland security concerns, DOD is not the lead agency, but has significant supporting roles in several areas (see Figure I-4). In homeland defense missions (air, land and maritime missions), DOD will take the lead and be supported by other Federal agencies. Section 876 of Public Law 107-296, the Homeland Security Act of 2002 states: "Nothing in this Act shall confer upon the Secretary [of Homeland Security] any authority to engage in warfighting, the military defense of the United States, or other military activities, nor shall anything in this Act limit the existing authority of DOD or the Armed Forces to engage in warfighting, the military defense of the United States, or other military activities."

d. DOD established United States Northern Command (USNORTHCOM) in 2002 to consolidate under a single unified command existing missions that were previously executed by other military organizations. The command's mission is homeland defense and civil support, specifically:

(1) Conduct operations to deter, prevent, and defeat threats and aggression aimed at the United States, its territories, and interests within the assigned AOR.

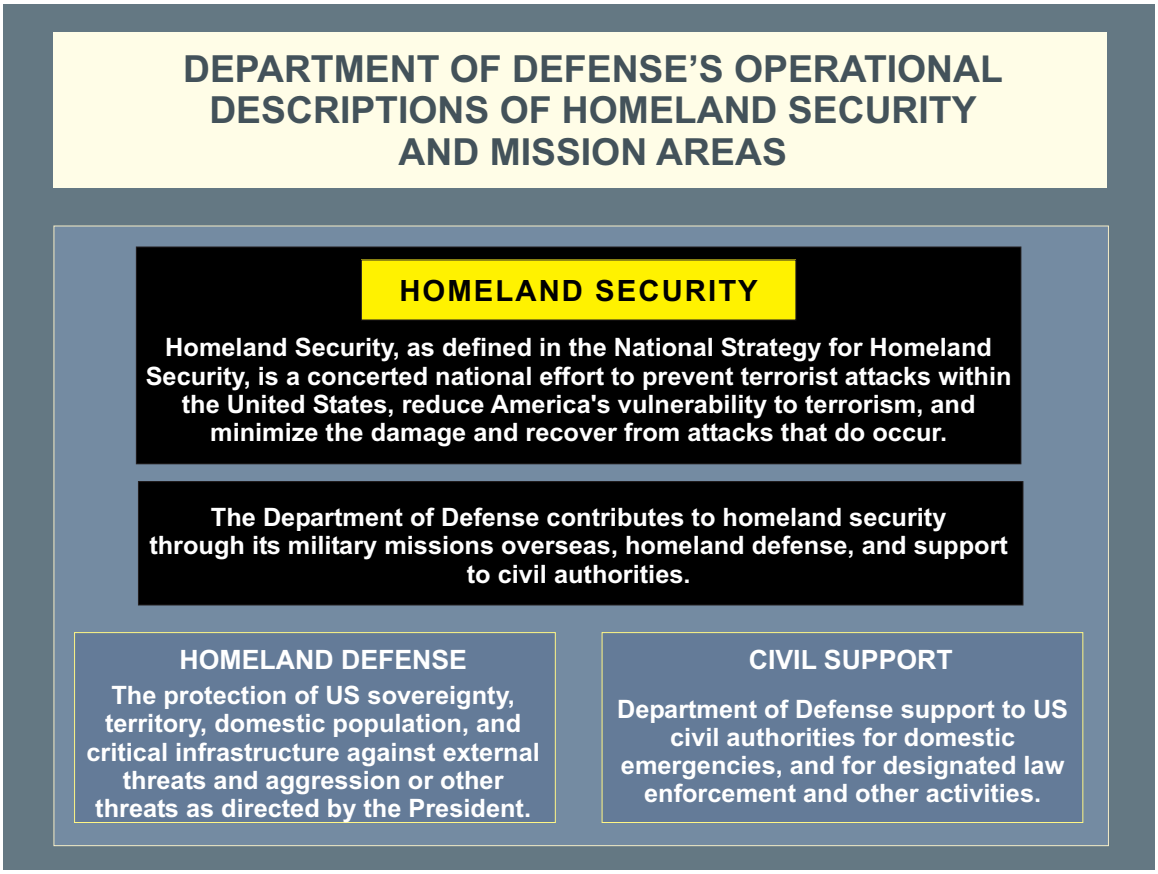


Figure I-4. Department of Defense's Operational Descriptions of Homeland Security and Mission Areas

(2) As directed by the President or SecDef, provide military assistance to civil authorities including CM operations.

(3) USNORTHCOM's AOR includes air, land, and sea approaches and encompasses the continental United States (CONUS), Alaska, Canada, Mexico, Puerto Rico, the US Virgin Islands, Bermuda, St. Pierre and Miquelon Islands, and waters out to 500 nautical miles (excluding Greenland and Siberia). The defense of Hawaii and our territories and possessions in the Pacific remains the responsibility of US Pacific Command.

CHAPTER II
TERRORIST THREAT

"Terrorism is an arm the revolutionary can never relinquish."

Carlos Marighella
MINIMANUAL OF THE URBAN GUERILLA

1. General

A critical factor in understanding terrorism is the importance of the emotional impact of the terrorist act on an audience other than the victim. This chapter provides an overview of issues dealing with the terrorist threat. The terrorist attacks of September 11, 2001, marked a dramatic escalation in trends toward more destructive terrorist attacks, showed the vulnerability of the United States, and the importance of preventing terrorism. The new terrorist paradigm includes traditional state sponsored terrorism, well organized networks of nonstate actors, extremist groups and criminal networks. Moreover, terrorists may act independently or in a well-orchestrated offensive.

2. Terrorist Tactics

The general shift in tactics and methodologies among international terrorists focuses on producing mass casualties. They have raised the stakes, operating now with a more fatalistic mentality and incorporating multiple simultaneous attacks and suicide bombings. Their targets may be just as likely economic (tourists, financial networks) or agricultural ones (livestock, crops) as embassies or military forces/facilities. Their goal is not just to win favor for their causes, but to wage undeclared, unconventional war at will. The more common tactics employed by terrorist groups are discussed below.

a. **Assassination.** A term generally applied to the killing of prominent persons and symbolic enemies as well as traitors who defect from the group.

b. **Arson.** Less dramatic than most tactics, arson has the advantage of low risk to the perpetrator and requires only a low level of technical knowledge.

c. **Bombing.** The improvised explosive device (IED) is the terrorist's weapon of choice. IEDs can be inexpensive to produce and, because of the various detonation techniques available, may be a low risk to the perpetrator. Suicide bombings, however, are a common attack method. Advantages to these tactics include their attention-getting capacity and the ability to control casualties through time of detonation and placement of the device. Announcing responsibility for the bombing or denying responsibility for the incident, should the action produce undesirable results, generates media interest and may lead to increased coverage of a terrorist group's agenda/activities.

d. **Hostage Taking.** This usually is an overt seizure of one or more individuals with the intent of gaining publicity, concessions in return for release of the hostages, or as human shields

to increase their success in carrying out a mission. While dramatic, hostage and hostage barricade situations are risky for the perpetrator.

e. **Kidnapping.** While similar to hostage taking, kidnapping has significant differences. Kidnapping is usually a covert seizure of one or more specific persons in order to extract specific demands. The perpetrators of the action may not be known for a long time. Because of the time involved, successful kidnapping requires elaborate planning and logistics. Because the perpetrator may not be known for a long time, the risk to the perpetrator is less than in the hostage situation.

f. **Hijacking or Skyjacking.** Sometimes employed as a means for escape, hijacking is normally carried out to produce a spectacular hostage situation or provide a vehicle for carrying out a lethal mission.

The American soldier is a symbol of US power and presence and is consequently a target for terrorists.

g. **Seizure.** Seizure usually involves a building or object that has value in the eyes of the intended audience. There is some risk to the terrorist because security personnel have time to react and may opt to use force to resolve the incident, especially if few or no innocent lives are involved.

h. **Raids or Attacks on Facilities.** Armed attacks on facilities are usually undertaken for one of three purposes: to gain access to radio or television broadcast capabilities in order to make a statement; to demonstrate the government's inability to secure critical facilities or national symbols; or to acquire resources (e.g., robbery of a bank or armory).

i. **Sabotage.** The objective in most sabotage incidents is to demonstrate how vulnerable society is to terrorist actions. Industrialized societies are more vulnerable to sabotage than less highly developed societies. Utilities, communications, and transportation systems are so interdependent that a serious disruption of any one affects all of them and gains immediate public attention. Sabotage of industrial or commercial facilities is one means of identifying the target while making a statement of future intent. Military facilities and installations, information systems, and information infrastructures may become targets of terrorist sabotage.

j. **Hoaxes.** Any terrorist group that has established credibility can employ a hoax with considerable success. A threat against a person's life causes that person and those associated

Port facilities may be one target of terrorist attacks.

with that individual to devote time and effort to security measures. A bomb threat can close a commercial building, empty a theater, or delay an aircraft flight at no cost to the terrorist. Repetitive or an inordinate number of false alarms may dull the analytical and operational efficiency of key security personnel, thus degrading readiness.

k. **Use of Weapons of Mass Destruction (WMD).** Terrorists have employed chemical and biological weapons in the past, and some terrorist organizations will seek to employ all types of CBRNE weapons when they can obtain them. These types of weapons, which are relatively cheap and easy to make, could be used in place of conventional explosives in many situations. The potential for mass destruction and the deep-seated fear most people have of chemical and biological weapons could be attractive to a group wishing to make the world take notice. Although an explosive nuclear device is acknowledged to be beyond the reach of most terrorist groups, a chemical or biological weapon or a radiological dispersion device using contaminants is not. The technology is simple and the cost per casualty (for biological weapons in particular) is extremely low — much lower than for nuclear explosives. This situation could change as the competition for headlines increases. Increasing availability of CBRNE material, components, and weapons raises the specter of terrorists using these weapons in an attack against civilian populations or military facilities. Many chemical-biological weapons ingredients are commercially available. Terrorists have attempted to obtain industrial radiological sources to be used in a "dirty bomb" scenario.

l. **Environmental Destruction.** Although this tactic has not been widely used, the increasing accessibility of sophisticated weapons to terrorists has the potential to threaten damage to the environment. Potential examples include intentional dumping of hazardous chemicals into the

public water supply, the destruction of oil tankers causing ecological harm, destroying oil fields, or poisoning a nation's food supplies. The use of exotic insects, animals, or plants to poison or destroy the food supply or ecosystem is a potential low cost terror weapon.

m. **Man-Portable Air Defense System (MANPADS).** Terrorists can use MANPADS to attack military or civilian aircraft. Terrorists have conducted such attacks previously, including an attack on a DHL cargo aircraft at Baghdad International Airport in November 2003.

3. Terrorist Groups

a. A terrorist group's selection of targets and tactics is also a function of the group's affiliation, level of training, organization, and sophistication. Security planners and terrorism analysts categorized terrorist groups according to their operational traditions — national, transnational, and international. National groups operated within the boundaries of a single nation. Transnational groups operated across international borders. International groups operated in two or more nations and were usually assumed to receive direction and support from a foreign government. Historically, terrorist groups have also been categorized by government affiliation to help security planners and terrorism analysts anticipate terrorist targets and their sophistication of intelligence and weaponry. Three general terrorist group categories are shown in Figure II-1.

b. While the three categories broadly indicate the degrees of sophistication that may be expected, it is important to examine each terrorist group on its own terms. The vast funds available to some narco-terrorists afford them the armaments and technology rivaling some nation-states. Religious cults or organizations have features from all three of the listed categories. They may be "nonstate-supported" (e.g., Japan's Aum Shinrikyo cult or Al-Qaeda), "state-supported" (e.g., extremist factions of Hamas who believe violence serves their concept of religious

Figure II-1. Categories of Terrorist Groups

servitude), or "state-directed" (e.g., Hizballah is both the "Party of God" and a religious organization that employs violence in support of both religion and politics).

c. Terrorism is essentially a network of networks comprised of extremist organizations, ideological motivated state and non state actors, and other opportunists who cooperate because of self interests. These opportunists, including criminals, organized criminal entities, proliferators, rogue states, insurgents, and others, are enablers to terrorists. They may not agree explicitly with the terrorists or their goals but expect to achieve some benefit or profit from their cooperation with the terrorists.

4. Terrorist Organizations

a. Terrorist organizations are not corporate or hierarchal, nor are they confined to borders. Groups may share considerable resources or only ideological goals. Out of necessity, the groups are generally resilient and adaptive to external pressures. Despite their diversity of motive, sophistication, and strength, these organizations share a conceptual structure as depicted in Figure II-2.

b. At the base, underlying conditions such as poverty, corruption, religious conflict, and ethnic strife create opportunities for terrorists to exploit. Some of these conditions are real and some manufactured. Terrorists use these conditions to justify their actions and expand their base of support. The belief that terror is a legitimate means to address such conditions and effect political change is a fundamental problem enabling terrorism to develop and grow. Passive supporters may not approve of a terrorist group's activities, but they do not get involved because of several possible reasons, including lack of trust or confidence in the government, fear of retribution, complete apathy, and lack of means for reporting activities confidentially.

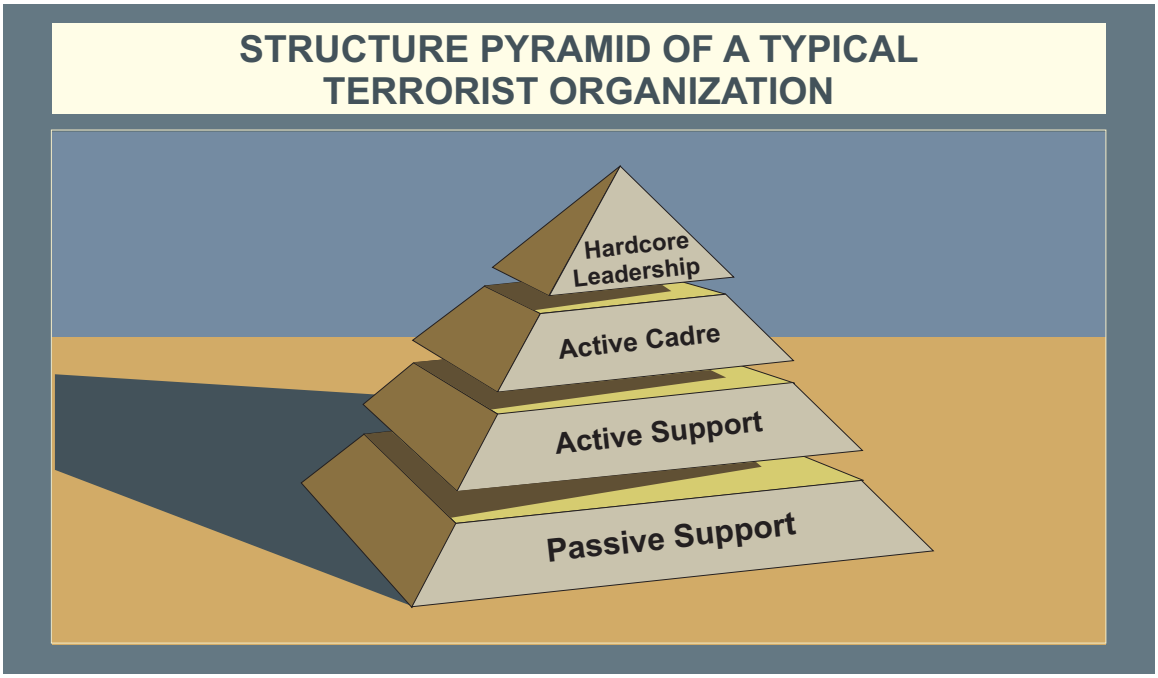


Figure II-2. Structure Pyramid of a Typical Terrorist Organization

c. The international environment defines the boundaries within which terrorists' strategies take shape. Porous borders as well as sympathetic governments provide terrorists access to havens, capabilities, and other support. Whether through ignorance, inability, or intent, states around the world still offer havens — both physical (e.g., safe houses, training grounds) and virtual (e.g., reliable communication and financial networks) — that terrorists need to plan, organize, train, and conduct their operations. Once entrenched in a safe operating environment, the organization can begin to solidify and expand. The terrorist organization's structure, membership, resources, supporters, and security determine its capabilities and reach.

d. Active support is the second largest and the most important level of a terrorist organization. Active supporters are critical to terrorist campaigns. Any group can carry out a bombing or kidnapping, but in order to sustain a campaign of bombings and kidnappings, the group must maintain active support. Active supporters keep the terrorists in the field. They maintain communication channels, provide safe houses, gather intelligence, and ensure all other logistical needs are met. This is the largest internal group in the organization.

e. The active cadre is responsible for carrying out the mission of the terrorist organization. Depending on the organization's size, each terrorist in the cadre may have one or more specialties. Other terrorists support each specialty, but the active cadre is the striking arm of the terrorist group.

f. At the top of the structure, the terrorist leadership provides the overall direction and strategy that link all these factors and thereby breathe life into a terror campaign. Hardcore terrorist leaders manipulate ideologies and philosophies for their own benefit. They selectively report information and disseminate 'news' in order to instill a sense of unity within the group, embrace disenfranchised individuals throughout a community, and ultimately consolidate and advance individual and group power. The leadership becomes the catalyst for terrorist action. The loss of the leadership can cause many organizations to collapse. Some groups, however, are more resilient and can promote new leadership should the original fall or fail. Still others have adopted a more decentralized organization with largely autonomous cells, making our challenge even greater.

g. While retaining this basic structure, the terrorist challenge has changed considerably over the past decade and likely will continue to evolve. Ironically, the particular nature of the terrorist threat faced today springs in large part from some of our past successes.

h. Al-Qaeda exemplifies how terrorist networks have twisted the benefits and conveniences of our increasingly open, integrated, and modernized world to serve their agenda. The Al-Qaeda network is a multinational enterprise with operations in more than 60 countries. Its camps in Afghanistan provided sanctuary and its bank accounts served as a trust fund for terrorism. Its global activities are coordinated through the use of personal couriers and communication technologies emblematic of our era — cellular and satellite phones, encrypted e-mail, Internet chat rooms, videotape, and CD-ROMs [compact disc read-only memory]. Like a skilled publicist, Usama bin Laden and Al-Qaeda have exploited the international media to project his image and message worldwide.

i. As the Al-Qaeda network demonstrates, the terrorist threat today is mutating into something quite different from its predecessors. Terrorists can now take full advantage of technology to disperse leadership, training, and logistics not just regionally but globally. Establishing and moving cells in virtually any country is relatively easy in a world where more than 140 million people live outside of their country of origin and millions of people cross international borders daily.

AL-QAEDA A.K.A Q'AIDAT AL-JIHAD "THE BASE"

Established by Usama Bin Ladin in the late 1980s to bring together Arabs who fought in Afghanistan against the Soviet Union. Helped finance, recruit, transport, and train Sunni Islamic extremists for the Afghan resistance. Current goal is to establish a pan-Islamic Caliphate throughout the world by working with allied Islamic extremist groups to overthrow regimes it deems "non-Islamic" and expelling Westerners and non-Muslims from Muslim countries, particularly Saudi Arabia. Issued statement under banner of "the World Islamic Front for Jihad Against the Jews and Crusaders" in February 1998, saying it was the duty of all Muslims to kill US citizens, civilian or military, and their allies everywhere. Merged with Egyptian Islamic Jihad (Al-Jihad) in June 2001.

Al-Qaeda probably has several thousand members and associates. Also serves as a focal point or umbrella organization for a worldwide network that includes many Sunni Islamic extremist groups, some members of al-Gama'a al-Islamiyya, the Islamic Movement of Uzbekistan, and the Harakat ul-Mujahidin.

Al-Qaeda has cells worldwide and is reinforced by its ties to Sunni extremist networks. Was based in Afghanistan until Coalition forces removed the Taliban from power in late 2001. Al-Qaeda has dispersed in small groups across South Asia, Southeast Asia, and the Middle East and probably will attempt to carry out future attacks against US interests.

Al-Qaeda maintains moneymaking front businesses, solicits donations from like-minded supporters, and illicitly siphons funds from donations to Muslim charitable organizations. US efforts to block Al-Qaeda funding has hampered the group's ability to obtain money.

SOURCE: United States Department of State
Patterns of Global Terrorism 2002
April 2003

j. Furthermore, terrorist groups have become increasingly self-sufficient by exploiting the global environment to support their operations. Whether it is the Revolutionary Armed Forces of Colombia's involvement in the cocaine trade in Colombia, Al-Qaeda's profiting from the poppy fields in Afghanistan, or Abu Sayyaf's kidnapping for profit in the Philippines, terrorists are increasingly using criminal activities to support and fund their terror. In addition to finding

sanctuary within the boundaries of a state sponsor, terrorists often seek out states where they can operate with impunity because the central government is unable to stop them. Such areas are found in the Americas, Europe, the Middle East, Africa, and Asia. Foreign terrorists also establish cells in the very open, liberal, and tolerant societies that they plan to attack.

5. Terrorism Against the Homeland

Terrorists have attacked within US borders ever since we gained our independence. Historically, though, the attacks were primarily committed by Americans, done infrequently, and on a generally small scale. Since the early 1990s, the scale of the attacks has increased, as has the presence of foreign terrorists (e.g., World Trade Center in 1993 and the attacks of September 11, 2001).

a. Securing the American homeland is a challenge of monumental scale and complexity. The 1995 bombing of the Murrah Federal Building in Oklahoma City and the attacks of 9/11 highlight the threat of terrorist acts within the US. Domestic terrorist groups, transnational terrorist groups, and special interest extremist groups continue to pose a threat to the peace and stability of our country.

b. Terrorists choose their targets deliberately based on the weaknesses they observe in our defenses and in our preparations. They can balance the difficulty in successfully executing a particular attack against the magnitude of loss it might cause. They can monitor our media and listen to our policymakers as our Nation discusses how to protect itself - and adjust their plans accordingly. Where we insulate ourselves from one form of attack, they can shift and focus on another exposed vulnerability. We must defend ourselves against a wide range of means and methods of attack. Terrorists continue to employ conventional means of attack, while at the same time gaining expertise in less traditional means, such as attacks on computer, banking, and utility systems. Other terrorists are working to obtain CBRNE weapons for the purpose of wreaking unprecedented damage on America.

c. Terrorist groups can infiltrate organizations, groups, or geographic areas to wait, watch, and identify weaknesses and opportunities while it is much more difficult for us to do the same. This trait is made even more relevant by our reliance on habitual processes such as repetitiveness in training and in our daily lives.

d. Military commanders are responsible to ensure that DOD resources are used as directed and consistent with laws, Presidential directives, executive orders (EOs), and DOD policies and directives,

See Joint Publication (JP) 3-26, Homeland Security*, for guidance in the conduct of homeland security operations.*

6. Asymmetric Tactics, Techniques, and Procedures

a. Terrorists have used a variety of tactics, techniques and procedures (TTP) to attack US forces. Because terrorists groups usually cannot confront US forces directly, they turn to asymmetric TTP. Although, the exact enemy TTP are constantly evolving, the National Ground Intelligence Center identified some overarching asymmetric TTP while reviewing Operation IRAQI FREEDOM (OIF) operations in the Spring 2004. However, these tactics can be employed in both expeditionary and nonexpeditionary environments.

b. Asymmetric TTP used in the OIF during the Spring 2004 were based on denial and deception, "human shield" tactics, "standoff" attacks, and IO. These TTP can be combined with conventional military tactics to serve as a battlefield multiplier.

(1) **Denial and Deception**

(a) Dispersing and Hiding. Dispersion and hiding in complex terrain such as cities deny US situational awareness and complicate targeting of precision fires. Urban areas offer excellent cover and concealment from US airpower because building interiors and subterranean areas are hidden from airborne observation and vertical obstructions hinder line of sight (LOS) to ground targets. C2 is often decentralized. Terrorist operations are nonlinear and dispersed.

(b) Exploitation of Sensitive Infrastructure. Urban infrastructure such as buildings, shrines, and ruins can be "sensitive" for political, religious, cultural, or historic reasons. Enemy forces deliberately occupy sensitive buildings under the assumption US forces will refrain from entering or returning fire.

(c) Terrorists also use police cars, taxis, and ambulances to move couriers, fighters, and ammunition. Terrorist forces have used civilian vehicles configured as vehicle borne improvised explosive devices (VBIEDs) as "technicals" to maneuver and fight, and as supply and transport vehicles. In one example, enemy forces reconfigured a white van with red crescents painted on the front and sides into a VBIED, which was detonated near a local hotel.

(2) **"Human Shields"**

(a) In their attacks, enemy forces deliberately use noncombatants as "human shields." This tactic forces coalition forces to adopt more stringent rules of engagement (ROE) and limit their heavy firepower capability.

(b) Supply civilians to the area of operations. In some areas, enemy forces prevented civilians from evacuating likely engagement areas in order to ensure that a source of human shields remained available. Elsewhere, subversives closed down schools and orchestrated work strikes to produce crowds of civilians in potential battle areas. Attackers have also used peaceful demonstrations as cover and a means of escape after execution of an attack.

(c) Maneuver within crowds of civilians. Terrorists use crowds of noncombatants to cover and conceal their movements and to negate coalition movements. In some cases, children were used as human roadblocks.

(d) Attack coalition targets from residential areas. Enemy forces have launched attacks from residential areas in order to invite coalition return fire into civilian homes.

(3) **Standoff Attacks**

(a) In general, enemy forces avoid or desire to limit their direct fire engagements with US heavy armored vehicles and prefer to conduct "standoff" attacks with IED bombs and indirect fire weapons. Standoff tactics permit the attack on a target with enough intervening distance and time to allow for escape from the engagement area and/or to avoid immediate overwhelming return fire by coalition units.

(b) Mortar "shoot and scoot" tactics. Mortars are the primary weapon of choice by enemy forces for applying "shoot and scoot" tactics in urban terrain. Attackers have mounted mortars in truck beds and inside of automobiles by cutting holes in the roofs of the car to fire the weapon. Attackers fire a few rounds from these systems before displacing (or scooting) to a new location. Enemy forces have also left these systems for capture after firing. Sometimes the equipment left behind is rigged with bombs or is targeted by another indirect firing system to engage unsuspecting coalition units who have captured the equipment.

(c) Mortars and their ammunition are available worldwide, are relatively easy to maintain, and are easy to employ. They are easy to hide, have high rates of fire, and can quickly

107 mm rocket "aimed" at Coalition Forces.

Vehicle borne improvised explosive device attack on coalition forces barely penetrated the perimeter but decimated the local neighborhood.

relocate. Mortars do not require large firing areas, and they are ideal for urban attacks as their arcing trajectory can clear high buildings. Rockets require more planning and more set-up time, but they increase attacker survivability and deliver a larger warhead.

(d) IEDs. Enemy forces have employed IED bombs from the simple small devices to massive 100 kilogram bombs buried in the road. Some of the most complex devices have included artillery shells "daisy-chained" together to explode along a section of the road over 100 meters long. Explosive charges have been placed in pipes, boxes, animal carcasses, piles of rocks, and any other innocuous object along the side of a road. Decoys and small IEDs have been used to draw coalition forces into kill zones for subsequent or secondary IED explosions.

(e) Conduct suicide-bomber attacks. Many suicide bomb attacks use VBIEDs. Multiple VBIEDs have also been employed, with the first vehicle explosion designed to open a breach into a hardened facility or perimeter barrier, and a second bomb to penetrate through the opening to attack the target.

(4) **IO**

(a) Enemy forces have used IO to disrupt popular support for coalition forces and to garner regional and international support for insurgent forces, mainly from Europe and the Islamic world.

(b) Spread rumors on the "street." Rumors have always been a powerful force. News from friends in marketplaces and cafes has always been used to offset the other official information. Enemy forces plant many rumors and initiate disinformation to discredit the coalition. For example, after a terrorist bombing, bystanders will often wave chunks of metal at film crews and claim they are shrapnel from US missiles and bombs. One rumor in OIF, which took months to disprove, was that the toys handed out by coalition soldiers caused deadly diseases in Iraqi children.

(c) Release favorable combat footage. Enemy forces rely heavily on video to distribute their propaganda. For example, crude digital video discs (DVDs) containing footage of attacks on coalition forces, wounded women and children, and damaged local infrastructure appeared in regional marketplaces immediately after attacks. DVDs usually praised the bravery of residents "who didn't submit to humiliation by the Americans," and include scenes depicting the bravery of fighters as they engage coalition troops.

(d) Post video on the Internet. Terrorist groups can use the Internet to disseminate its message as quickly as events happen. An immediate press release from a web site is not only cheap but offers direct control over the content of the message. Sites are managed to manipulate images in support of the resistance and to create special effects or deception.

(e) Ensure media access to the battlefield. Enemy forces use sympathetic media to reinforce their IO plan. Some media companies repeatedly display images of casualties, massive collateral damage, and the accusation that coalition forces use excessive force.

(f) Attacks on local government officials and civilians. This tactic avoids the strength of American military forces and concentrates on the various levels of the public servants and innocent civilians. In the conduct of such attacks, the terrorists are undermining the government's efforts to maintain stability and attempting to intimidate other individuals from supporting or assisting the government. In the case of attacks on the civilians, the murders can be filmed and distributed as mentioned above.

CHAPTER III
INTELLIGENCE, COUNTERINTELLIGENCE, THREAT ANALYSIS, AND COUNTERSURVEILLANCE

"We made mistakes. Our failure to watchlist Al Hamzi and Al Midhar in a timely manner — or the FBI's inability to find them in the narrow window of time afforded them — showed systemic weaknesses and the lack of redundancy."

Written Statement for the Record of the Director of Central Intelligence Before the National Commission on Terrorist Attacks Upon the United States, April 14, 2004.

1. Intelligence and Counterintelligence

a. **Intelligence and Counterintelligence Support.** Intelligence and CI are critical in the development of an AT program. Strategic, well-planned, proactive, systematic, all-source intelligence, and CI programs are essential. The role of intelligence and CI is to identify, assess, deter, disrupt, and defeat the threat, provide advance warning, and disseminate critical information/ intelligence in a usable form for the commander. Effective intelligence and CI support requires effort to execute the intelligence process and to conduct effective operations and investigations against the threat. The entire process is important in providing decision makers with information and timely warnings upon which to recommend FP actions.

b. **Sources.** The primary sources of intelligence and CI for the AT program are open-source information; local, state, and Federal LE information; US intelligence; information shared through liaison with foreign governments; local information; and military source operations in some overseas deployed environments (see Figure III-1).

See JP 2-01.2, Counterintelligence and Human Intelligence Support to Joint Operations.

(1) **Open-Source Information.** This information is publicly available and can be collected, retained, and stored by the Intelligence Community in accordance with DOD 5240.1-R, *Activities of DOD Intelligence Components that Affect United States Persons*. DODD 5200.27, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense*, also pertains. The news media are excellent open sources of information on terrorism. The news media report many major terrorist incidents and often include in-depth reports on individuals, groups, or various government counterstrategies. Government sources include congressional hearings; publications by the Defense Intelligence Agency (DIA), the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and DOS; and the national criminal justice reference services. Additionally, there are private data services that offer timely information on terrorist activities worldwide. Terrorist groups and their affiliates may also have manuals, pamphlets, and newsletters that reveal their objectives, tactics, and possible targets. Open sources are not a substitute for classified capabilities, but they can provide a valuable foundation and context for rapid orientation of the analyst and the consumer and for the establishment of collection requirements which take full advantage of the unique access provided by classified sources.

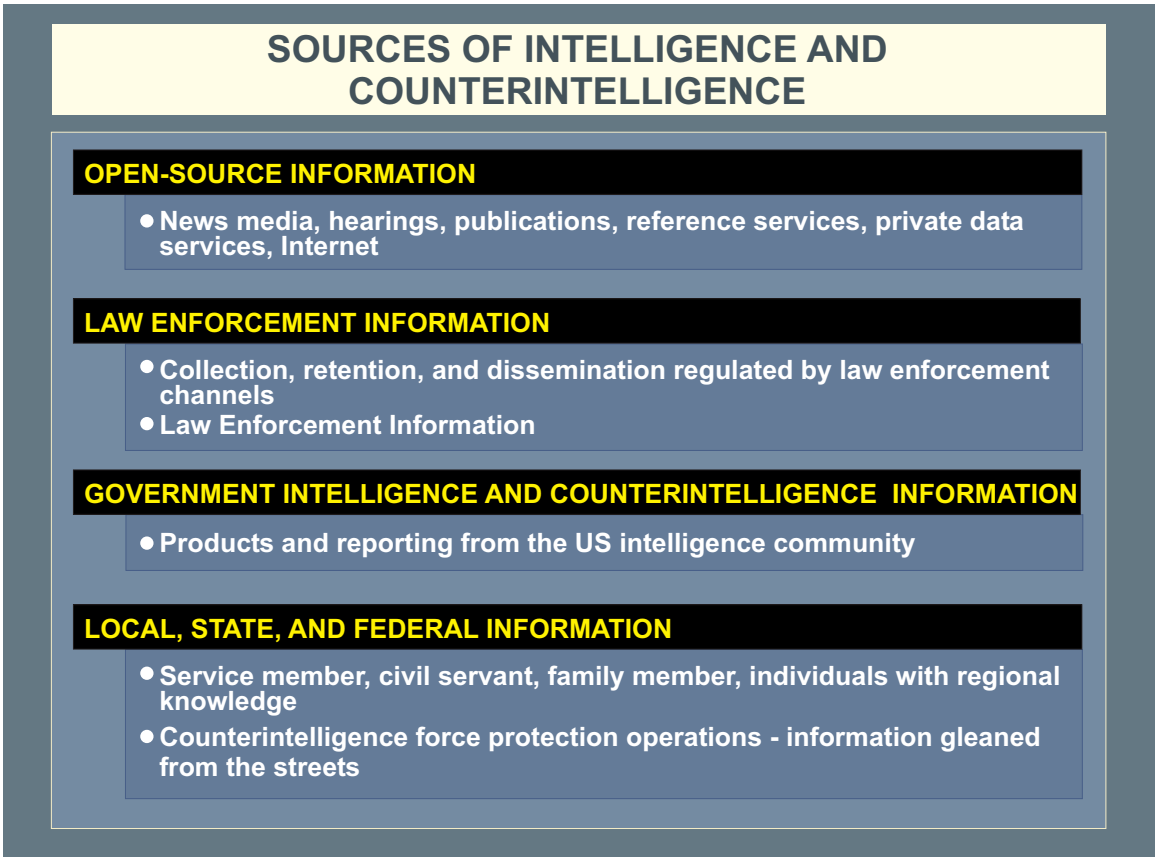


Figure III-1. Sources of Intelligence and Counterintelligence

(2) **Law Enforcement Information.** Both military and civil law enforcement agencies (local, state, and Federal) have access to criminal records. Because terrorist acts are criminal acts, criminal records are a major source for terrorist intelligence. Commanders must work through established LE liaison channels because the collection, retention, and dissemination of criminal records are regulated. Local military criminal investigative offices of the US Army Criminal Investigations Command (USACIDC), Naval Criminal Investigative Service (NCIS), Air Force Office of Special Investigations (AFOSI), and Headquarters, US Marine Corps, Criminal Investigations Division, maintain current information that will assist in determining the local terrorist threat. See DODD 5200.27, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense*, on proper handling of this information.

(3) **Government Intelligence.** The Community Counterterrorism Board, which manages the Interagency Intelligence Committee on Terrorism under the Director of Central Intelligence, is the organization that links all 60-plus Federal intelligence, defense, and civilian agencies involved in counterterrorism. These agencies include the CIA (lead agency), DIA, National Security Agency, National Geospatial-Intelligence Agency, DOS, Department of Justice (DOJ), FBI, the Department of Energy, the Department of Transportation, United States Coast Guard (USCG), Federal Aviation Administration, Federal Communications Commission, Department of Homeland Security (DHS), and DOD. In response to the terrorist attacks of September 11, 2001 and subsequent Congressional inquiries into the intelligence process,

significant changes to the national intelligence structure have emerged. One change was the creation of the National Counterterrorism Center, which merges and analyzes terrorist-related information collected domestically and abroad in order to form the most comprehensive possible threat picture. It includes DOD representation. Lastly, the FBI has a national Joint Terrorism Task Force (JTTF) which includes nearly 30 agencies, spanning the fields of intelligence, public safety, and Federal, state, and local LE. The National JTTF collects terrorism information and intelligence and funnels it to the 66 local and state JTTFs. The DOD is represented at the national level and many of the state and local JTTFs have Service representation from nearby military installations. Service intelligence and CI production organizations that compile comprehensive intelligence and CI from these agencies for distribution on a need-to-know basis throughout the Services include: the Army Counterintelligence Center; the Navy Multiple Threat Alert Center; Headquarters, Marine Corps Intelligence Activity, AFOSI. In combatant commands, the intelligence directorate of a joint staff (J-2) is responsible for the integration of intelligence policy issues, developing detailed intelligence plans, integrating national and theater intelligence support, and ensuring accessibility of intelligence. The counterintelligence staff officer (CISO) provides CI interface among the combatant command, the component commands, and the joint staff.

(4) **Local, State, and Federal Information.** Other valuable sources of information are the individual Service member, civil servant, family member, and individuals with regional knowledge such as college faculty or members of cultural organizations. Local crime or neighborhood watch programs can also be valuable sources of information and can serve as a means to keep individuals informed in dispersed and remote areas. Intelligence exchanges with local government agencies through cooperative arrangements can also augment regional information.

c. **Responsibilities of Intelligence Agencies and Activities**

(1) **General.** The FBI is responsible for collecting and processing terrorist information to protect the United States from terrorist attack. Overseas, terrorist intelligence is principally a CIA responsibility, but the DOS, DIA, and HN are also active players. Military intelligence activities are conducted in accordance with Presidential EOs, Federal law, status-of-forces agreements (SOFAs), MOUs, and applicable Service regulations.

(2) **Intelligence Activities**

(a) The combatant commander, through the J-2, joint intelligence center, the CISO, and in consultation with DIA, CIA, US country team, and applicable HN authorities, obtains intelligence and CI information specific to the operational area and issues intelligence and CI reports, advisories, and assessments. This network is the backbone for communicating intelligence and CI information, advisories, and warning of terrorist threats throughout the region.

(b) DODD 2000.12, *DOD Antiterrorism (AT) Program*, tasks the Secretaries of the Military Departments to ensure Service component commands have the capability to collect, receive, evaluate, analyze, and disseminate all relevant data on terrorist activities, trends, and

indicators of imminent attack, and to develop the capability to fuse suspicious activity reports from military security, LE, and CI organizations with national-level ISR collection activities.

(c) DODD 5105.67, *Department of Defense Counterintelligence Field Activity (DOD CIFA)*, 2/19/2002 tasks the Secretaries of the Military Departments to:

1. Support the DOD Counterintelligence Field Activity (CIFA) in implementing Presidential Decision Directive/National Security Council-75, *US Counterintelligence Effectiveness, Counterintelligence for the 21st Century*, December 28, 2000, in integrating the Defense Counterintelligence Program DOD-wide, and in overseeing the appropriate functional aspects of the program.

2. Report all significant CI activities, including investigations and operations, to the Director, DOD CIFA.

(d) DOD CIFA Antiterrorism Responsibilities:

1. Establish a threat analysis capability designed to collect, fuse, and analyze domestic LE information with foreign intelligence and CI information in support of the DOD CbT mission. As a designated DOD LE and CI activity, CIFA shall support the efforts of the DIA Joint Intelligence Task Force for Combating Terrorism (JITF-CT), serving as the bridge between intelligence related to international terrorism and domestic LE information.

2. Support the JITF-CT, the combatant commands, DOD agencies, and the Military Services in preparing TAs and advisories.

3. Conduct specific risk assessments in support of the DCIP. Identify and maintain a database of critical DOD assets and infrastructure. This database shall include vulnerability assessments of all DOD facilities.

4. Support DOD CI components in preparing TAs by providing tailored analytical and data-mining services.

5. Assign DOD CI and criminal investigative personnel to the National Joint Terrorism Task Force and designated JTTFs within CONUS. Provide program oversight and coordination for assigned CI assets and serve as the repository for information obtained.

6. Provide countersurveillance support to the combatant commands upon request, subject to the approval of the CJCS.

7. Provide a member to the DOD ATCC and subcommittees as required.

8. Assist the DIA in the execution of its diplomatic security function. Such assistance shall include:

a. Representation at the National Security Council's Overseas Security Policy Board and other related committees, subcommittees, and working groups.

b. Support the DIA security assistance visits and vulnerability assessments for all DOD elements under the security responsibility of the COMs.

(e) Each Military Department intelligence agency is responsible for the following:

1. Provide overall direction and coordination of the Service CI effort.

2. Operate a 24-hour operations center to receive and disseminate worldwide terrorist threat information to and from the combatant command J-2s, applicable Service staff elements, subordinate commands, and national agencies.

3. Provide Service commanders with information on terrorist threats concerning their personnel, facilities, and operations.

4. With the FBI or HN authorities, investigate terrorist incidents for intelligence, CI, and FP aspects.

5. Provide terrorist threat information in threat briefings.

6. Conduct liaison with representatives from Federal, state, and local agencies as well as HN agencies to exchange information on terrorists.

7. Provide international terrorism summaries and other threat information to supported commanders. On request, provide current intelligence and CI data on terrorist groups and disseminate time-sensitive and specific threat warnings to appropriate commands.

(f) Investigative Agencies. Service criminal investigative services (e.g., USACIDC, NCIS, AFOSI) collect and evaluate criminal information and disseminate terrorist-related information to supported installation and activity commanders as well as to the Service lead agency. As appropriate, criminal investigative elements also conduct liaison with local military police or security personnel and civilian LE agencies.

(g) Intelligence staff elements of commanders at all echelons will:

1. Promptly report all actual or suspected terrorist incidents, activities, and early warnings of terrorist attack to supported and supporting activities, the local CI office, and through the chain of command to the Service lead agency.

2. Initiate and maintain liaison with the security personnel or provost marshal's office, local military criminal investigative offices, local CI offices, security offices, HN agencies, and (as required or allowed by law or policy) other organizations, elements, and individuals.

3. In cooperation with the local CI offices, develop and present terrorism threat awareness briefings to all personnel within their commands.

(h) LE, military police, and security personnel staff elements will be responsible for the following:

1. Report all actual or suspected terrorist incidents or activities to their immediate commander, supported activities, and Service lead agency through established reporting channels.

2. Initiate and maintain liaison with local CI offices and military criminal investigative offices.

3. Maintain liaison with Federal, HN, and local LE agencies or other civil and military AT agencies as appropriate and as provided in Service or agency regulations.

An improvised 2.75in rocket launcher among captured munitions from a terrorist cache.

(i) Installation, base, ship, unit, and port security officers will be responsible for the following:

1. Report all actual or suspected terrorist incidents or activities to their immediate commander, supporting military LE office, other supported activities, local CI office, and local military criminal investigation office.

2. Conduct regular liaison visits with the supporting military LE office, CI office, and local criminal investigation office.

3. Coordinate with the supporting military LE office and CI offices on their preparation and continual updating of the TAs.

4. Assist in providing terrorism threat awareness training and briefings to all personnel and family members as required by local situations.

(j) Services, DOD agencies, and resident combatant commander installations in the US should submit Threat and Local Observation Notices (TALONs) and other suspicious activity reports into the Joint Protection Enterprise Network within 24 hours of an event occurring.

d. **Information Requirements.** To focus threat analysis, the intelligence staff uses the commander's designated priority intelligence requirements (PIRs) to develop information requirements (IRs) for identifying and categorizing potential terrorist targets based on existing knowledge of an organization. Terrorist group IRs are shown in Figure III-2.

2. Threat Analysis

a. Terrorism threat analysis is a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups or individuals that could target the DOD components, elements, and personnel. A threat analysis shall review the factors of a terrorist group's operational capability, intentions, and activity, as well as the operating environment within which friendly forces operate. Threat analysis is an essential step in identifying and describing the threat posed by specific terrorist group(s) and/or individuals in a terrorism TA. A vulnerability assessment is an evaluation to determine the vulnerability to a terrorist attack against an installation, unit, exercise, port, ship, residence, facility, or other site. The TA and VA are then utilized with the criticality assessment to provide the basis for risk management decisions. Commanders must determine which assets require the most protection and where future expenditures are required to minimize risk of attack or lessen the severity of the outcome of an attack. To enhance this capability, which requires the collection and analysis of information from many sources, DIA currently maintains a DOD terrorism knowledge database and is developing a terrorism web site. The combatant command's J-2, the CISOs, in consultation with DIA, focuses this database information and regional information toward the intelligence and CI needs specific to the security of the command. Country TAs and information about terrorist organizations, biographies, and incidents in the database are disseminated to the commands and Services. Commands at all echelons then augment or refine the DIA's analyses to focus on their area of interest. This process is operative across the range of military operations, promotes coordination between all levels of the intelligence, CI, and LE communities, and enhances timely distribution of information to the supported commander.

(1) Several factors complicate intelligence and CI collection and operations. The small size of terrorist groups, coupled with their mobility and cellular organization, make it difficult to identify the members. Unlike other criminals, terrorist cadres often receive training in CI, OPSEC, and security measures from foreign intelligence agencies or other terrorists. AT requires additional proactive efforts that integrate the traditional LE measures with more tactical intelligence and CI analysis. AT officers and analysts may want to maintain a threat information organization plan that systematically outlines threats and threat indicators. A sample threat information organization plan is available through the Joint Antiterrorism Program Manager's Guide (JAT Guide) available at www.atep.smil.mil and a separate example is attached in Appendix L, "Threat Information Organization Matrix."

(2) The ability of an intelligence system to provide critical and timely information to the user depends not only on efficient collection and processing, but also on the ability to organize, store, and rapidly retrieve this information. This capability, coupled with early warning, careful observation, and assessment of threat activity, enhances the probability of accurately predicting the types and timing of terrorist attacks.

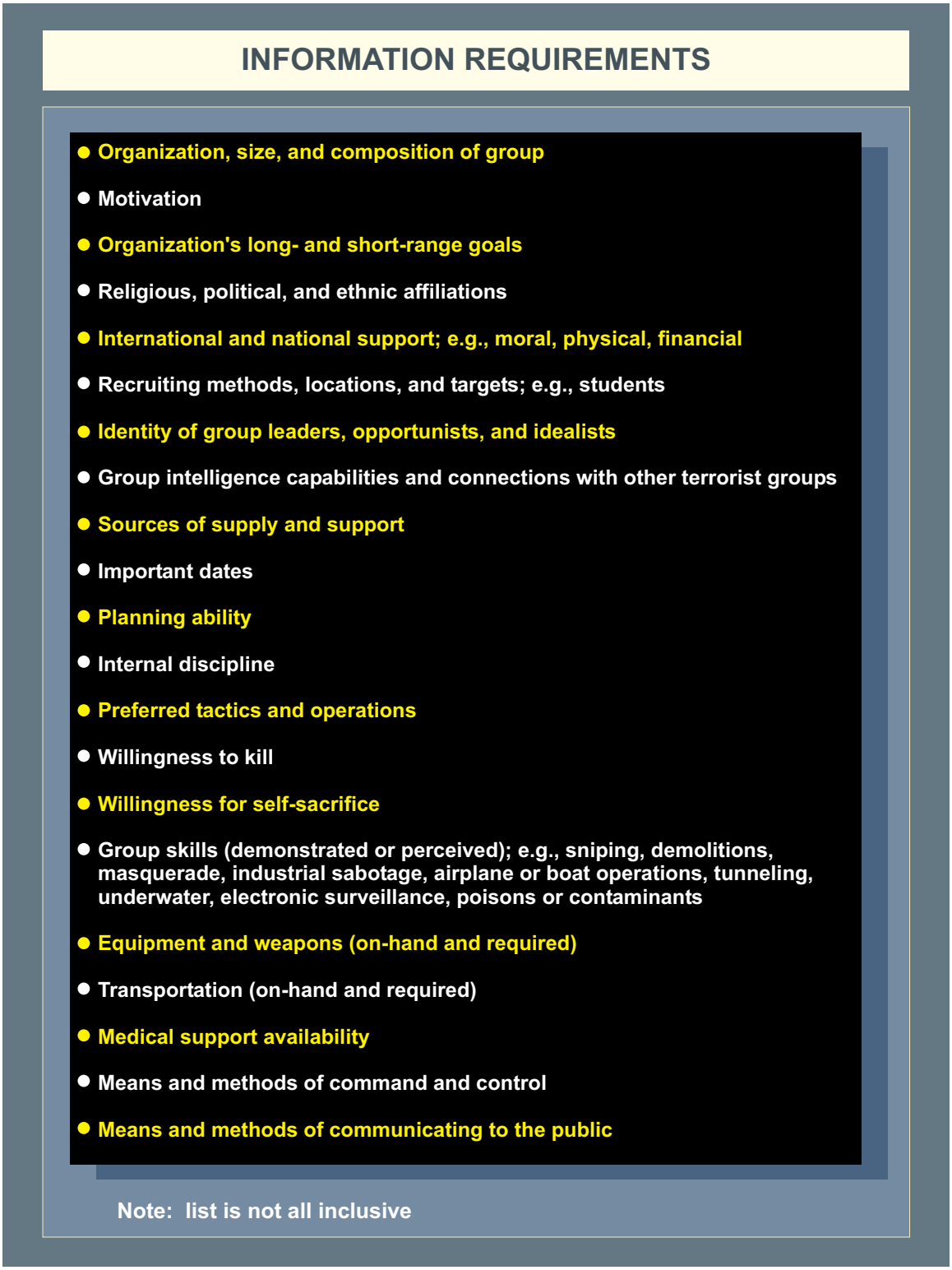


Figure III-2. Information Requirements

(3) Commanders must carefully exercise judgment in estimating both the existing terrorist threat and the need for changes in AT measures. See Appendix B, "Threat Assessment."

b. The commander and staff must first complete a criticality assessment (Appendix A, "Criticality Assessment") to identify the vital assets they need to perform their mission. Then they should proceed to complete the TA (Appendix B, "Threat Assessment") and then the vulnerability assessment (Appendix C, "Vulnerability Assessment").

c. **Drills and Exercises.** Multi-echelon wargaming of possible terrorist attacks is the best test, short of an actual incident, to analyze the ability of an installation, base, ship, unit, airfield, or port to respond. Drills and exercises test suspected vulnerabilities and AT measures. These exercises and drills also train the staff as well as reaction force leadership and help maintain a valid TA by identifying and adjusting to changing threat capabilities as well as known vulnerabilities.

3. Countersurveillance

a. Countering terrorist surveillance successfully necessitates commanders and security planners understand the purpose of terrorist surveillance, know what terrorists look for, and know how they conduct surveillance operations. With this basic knowledge, commanders can then implement protective countermeasures, comply with DOD standardized reporting procedures, and in the end deter, detect, disrupt, and defend against future attacks.

b. **Vulnerability Assessment.** Terrorists conduct surveillance to determine a target's suitability for attack by assessing the capabilities of existing security systems and discerning weaknesses for potential exploitation. Terrorists closely examine security procedures, such as shift changes, access control, and roving patrols; citizenship of security guards; models and types of locks; presence of closed-circuit cameras; and guard dogs. After identifying weaknesses, terrorists plan their attack options at the point or points of greatest vulnerability.

c. **Terrorist Surveillance Techniques.** The basic methods of surveillance are "mobile" and "fixed" (or static).

(1) Mobile surveillance entails active participation by the terrorists or operatives conducting surveillance, usually following as the target moves. Terrorists conduct mobile surveillance on foot, in a vehicle, or by combining the two. Mobile surveillance usually progresses in phases from a stakeout, to a pick up, and then through a follow phase until the target stops. At this point, operatives are positioned to cover logical routes to enable the surveillance to continue when the target moves again.

(2) Terrorists conduct fixed or static surveillance from one location to observe a target, whether a person, building, facility, or installation. Fixed surveillance often requires the use of an observation point to maintain constant, discreet observation of a specific location. Terrorists establish observation posts in houses, apartments, offices, stores, or on the street. A mobile surveillance unit, such as a parked car or van, can also serve as an observation post. Terrorists often park outside a building, facility, or installation to observe routines of security and personnel coming and going. Terrorists also use various modes of transportation to include buses, trains, or boats or move by foot to approach and observe installations.

The emphasis of surveillance detection is on indicators and warnings of terrorist surveillance activities.

d. **Protective Countermeasures.** The incorporation of visible security cameras, motion sensors, working dog teams, random roving security patrols (varying size, timing, and routes), irregular guard changes, and active searches (including x-ray machines and explosive detection devices) of vehicles and persons at entry points will improve situational awareness and present a robust force protection posture that dramatically inhibits terrorist surveillance efforts. The emplacement of barriers, roadblocks, and entry mazes that are covered by alert security personnel will provide additional deterrence as these measures increase standoff and improve security personnel reaction time in the event of an attack. The implementation of unannounced random security measures such as 100% identification of all personnel entering the facility / installation, conducting inspections and searches of personnel and vehicles, and visible displays of vehicles mounted with crew served weapons will increase uncertainty and thus the risk of failure in the minds of terrorists.

e. **Surveillance Detection.** Because terrorists conduct surveillance — often over a period of weeks, months, or years — detection of their activities is possible. Regardless of the level of expertise, terrorists invariably commit mistakes. Knowing what to look for and to be able to distinguish the ordinary from the extraordinary are keys to successful surveillance detection. For these reasons, overt surveillance detection in its most basic form is simply watching for persons observing personnel, facilities, and installations.

(1) The objectives of overt surveillance detection measures are to record the activities of persons behaving in a suspicious manner and to provide this information in a format useable by the appropriate LE or intelligence officials. It is important to note that overt surveillance

detection emphasizes the avoidance of interpersonal confrontations with suspicious individuals unless exigent situations necessitate otherwise. Depending upon the circumstances or trends, commanders and senior LE officials in coordination with intelligence experts through installation threat working groups may determine the need for more specialized covert countersurveillance measures to assure installation protection.

(2) For surveillance detection efforts to achieve positive results, military police/security personnel should immediately report incidents of surveillance and suspicious activities by providing detailed descriptions of the people, the times of day, the locations, the vehicles involved, and the circumstances of the sightings to their respective criminal investigative services or counterintelligence elements for incorporation into reports such as Air Force TALON or the Naval Criminal Investigative Service Suspicious Incident Report. The incident reports are important pieces of information that over time, combined with other similar sightings, allow investigators to assess the level of threat against a specific facility, installation, or geographic region. Such reports should be submitted to the Joint Protection Enterprise Network within 24 hours of an event occurring.

(3) The emphasis of surveillance detection is on indicators and warnings of terrorist surveillance activities. Surveillance detection efforts should focus on recording, then reporting incidents similar to the following:

(a) Multiple sightings of the same suspicious person, vehicle, or activity, separated by time, distance, or direction.

(b) Possible locations for observation post use.

(c) Individuals who stay at bus/train stops for extended periods while buses/trains come and go.

(d) Individuals who conduct inordinately long conversations on pay or cellular telephones.

(e) Individuals who order food at a restaurant and leave before the food arrives or who order without eating.

(f) Joggers who stand and stretch for an inordinate amount of time.

(g) Individuals sitting in a parked car for an extended period of time.

(h) Individuals who don't fit into the surrounding environment by wearing improper attire for the location (or season).

(i) Individuals drawing pictures / taking notes in an area not normally of interest to a standard tourist or showing interest in or photographing security cameras, guard locations, or noticeably watching security reaction drills and procedures.

(j) Individuals who exhibit unusual behavior such as staring or quickly looking away from individuals or vehicles as they enter or leave designated facilities or parking areas.

(k) Terrorists may also employ aggressive surveillance by false phone threats, approaching security checkpoints to ask for directions, or "innocently" attempting to smuggle nonlethal contraband through checkpoints. Clearly, the terrorists intend to determine firsthand the effectiveness of search procedures and to gauge the alertness and reaction of security personnel.

(4) It is important to highlight that the above surveillance indicators are recorded overtly and while performing normal military police/security personnel activities. The intent is to raise the awareness of our military police/security personnel to record and report the unusual during the course of routine LE and security duties.

f. **Reporting Terrorist Surveillance Indicators.** Implementing effective security countermeasures and employing overt surveillance detection principles will deter terrorist surveillance. However, regardless of the capabilities of a facility or installation to resource AT protective measures, good working relationships with local, state, and Federal law enforcement agencies are essential to establishing cohesive, timely, and effective responses to the indicators of terrorist activity. Commanders should coordinate and establish partnerships with local authorities (i.e., installation threat working groups) to develop intelligence and information sharing relationships to improve security for the installation and the military community at large. For those occasions when the indicators of terrorist surveillance continue despite well executed overt security countermeasures the objectives should be to provide detailed reports of the indicators of surveillance to the appropriate LE agency or intelligence activity. As reports of suspicious activity increase and the trends clearly indicate preoperational terrorist surveillance, it may be necessary for commanders in coordination with senior LE and intelligence officials to implement more sophisticated, uniquely-tailored countersurveillance solutions and assets to investigate the circumstances. Specialized countersurveillance assets should be coordinated and vetted by forwarding requests through the chain of command via predetermined Service or combatant command request procedures.

4. Threat Levels

Discussions of threat level determination, threat level assessments, and threat warnings can be found in DOD O-2000.12H, *DOD Antiterrorism Handbook*, Chapter 5.

CHAPTER IV
LEGAL CONSIDERATIONS

"To defeat terrorists we will support national and partner nation efforts to deny state sponsorship, support, and sanctuary to terrorist organizations. We will work to deny terrorists safe havens in failed states and ungoverned regions. Working with other nations' military and other governmental agencies, the Armed Forces help to establish favorable security conditions and increase the capabilities of partners. The relationships developed in these interactions contribute to a global antiterrorism environment that further reduces threats to the United States, its allies, and its interests.

National Military Strategy of the United States of America, 2004

1. General

This chapter explains the importance and necessity for participation of a command judge advocate at all levels of foreign and domestic AT program planning and implementation. It is designed to provide to commanders with a basic understanding of relevant legal considerations in implementing an AT program. The policy and jurisdictional responsibilities generally applicable to the Armed Forces of the United States are outlined below.

2. Commander's Authority

Commanders have the responsibility and inherent authority to enforce security measures and to protect persons and property under their control. Commanders should consult with their legal advisors often when establishing their AT programs. Legal personnel should be members of all installation or unit AT cells, boards, and working groups.

3. Limits of Military Support to Civil Authorities

a. **General.** DOD is the lead, supported by other agencies, in defending against traditional external threats/aggression against the US homeland. However, against internal, asymmetric, or nontraditional threats (e.g., terrorism), DOD may be in support of DHS or another lead or primary agency.

b. **Support to Civil Authorities.** When providing support to civil authorities, DOD will do so as directed by the President or the SecDef and consistent with laws, Presidential directives, EOs, and DOD policies and directives. The following general principles apply to such support:

(1) DOD resources should only be provided when response or recovery requirements are beyond the capabilities of local, state, and Federal civil authorities, and, except for narrow circumstances, only when approved by SecDef (see Figure IV-1). Military commanders may provide immediate response assistance under the appropriate circumstances without prior SecDef approval. In certain circumstances, **imminently serious conditions resulting from either civil emergencies or attacks may require immediate response by military commanders**.

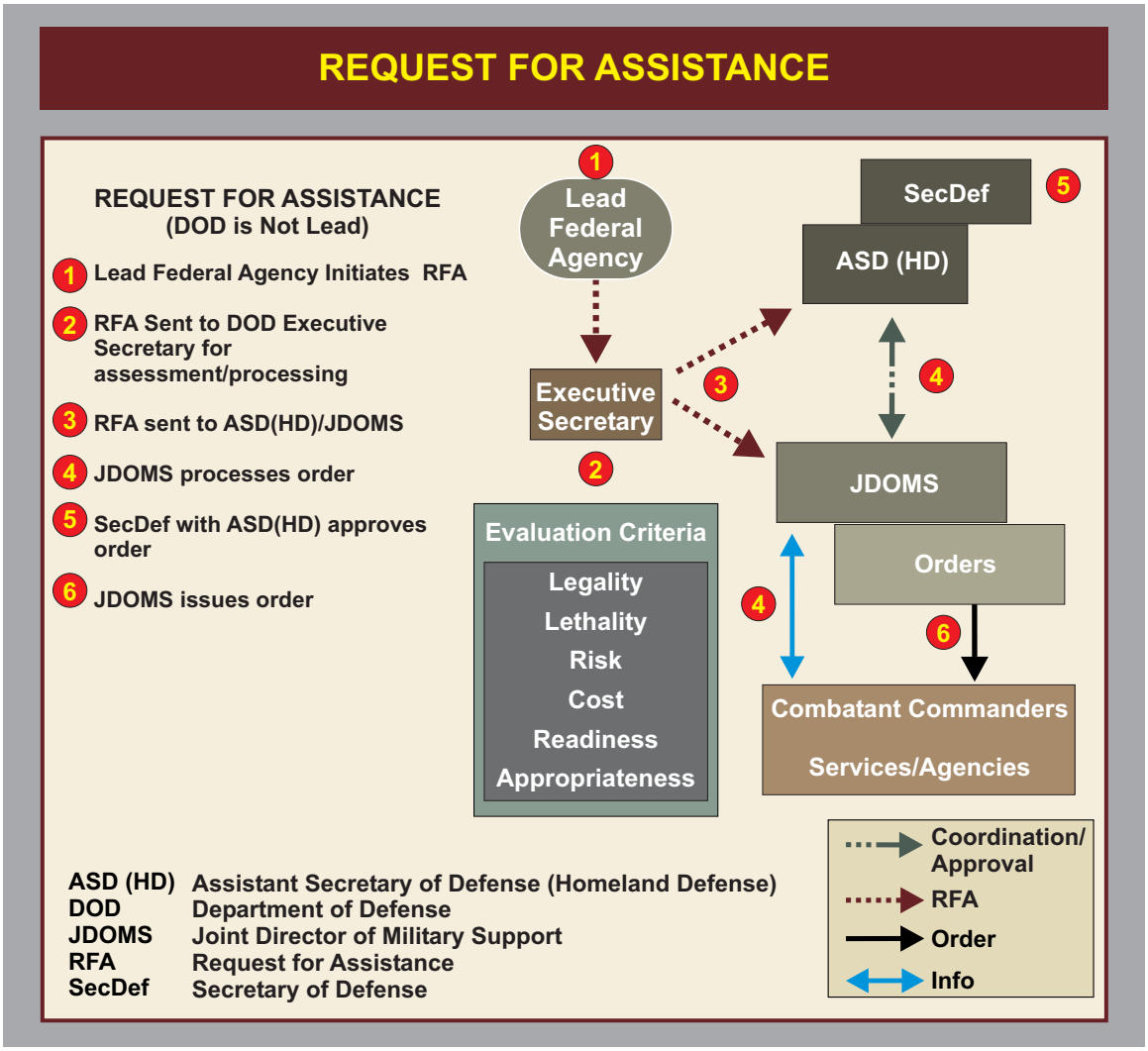


Figure IV-1. Request for Assistance

Responses to requests from civil authorities prior to receiving authority from the President or chain of command are made when immediate support is critical **to save lives, prevent human suffering, or mitigate great property damage**. When such conditions exist and time does not permit prior approval from higher HQ, commanders or officials acting under immediate response authority may take necessary action to respond, but must advise the DOD Executive Secretary (EXECSEC) through command channels by the most expeditious means available and seek approval or additional authorizations. The EXECSEC will notify SecDef, CJCS, and any other appropriate officials. The military will begin disengagement from immediate response activity as soon as practicable. While immediate response should be provided to civil agencies on a cost-reimbursable basis if possible, it should not be delayed or denied because of the inability or unwillingness of the requester to make a commitment to reimburse DOD.

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

(2) SecDef shall retain control of Title 10, United States Code (USC) military forces providing support. The dual Federal-state mission of the National Guard (NG), organized under the supervision of the adjutant general and the direction of the governor in each state/territory, makes it likely that the NG will be the first military responder during a support event. This early employment of NG will be in a state status (state active duty or Title 32) under the direction of the governor, and generally in advance of a formal Federal response request being generated. There are advantages associated with employment of the NG in state status, most notably no Posse Comitatus Act (PCA) constraints.

(3) Unless otherwise directed by SecDef, or where provided for by law, military operations will have priority over support to civil authorities.

c. **Posse Comitatus Act** (Title 18, USC, Section 1385). This Federal statute places limits on the use of military personnel for LE. The PCA prohibits direct, active use of federal military personnel to enforce civilian laws, except as authorized by the US Constitution or an act of Congress. Although the PCA, by its terms, refers only to the US Army and US Air Force, DOD policy extends the prohibitions of the act to US Navy and US Marine Corps as well. There are a number of exceptions to the PCA, including:

(1) NG forces operating under state active duty or Title 32, USC status.

(2) Federal troops acting pursuant to the Presidential power to quell insurrection (Title 10, USC, Sections 331-334).

(3) Assisting DOJ in cases of offenses against the President, Vice President, members of Congress, or a Supreme Court Justice (18 USC Sections 1751 and 351 respectively).

(4) Statutorily-allowable support to LE agencies (Title 10, USC, chap 18).

(5) The USCG when operating under Title 14, USC, authority.

(6) Response to emergency situations involving chemical or biological WMD (Title 10, USC, Section 382).

d. Sound legal advice will ensure that the application of military capabilities and resources properly considers legal constraints and restraints. Although statutory exceptions allow the use of military forces in some contexts, prior to committing forces, commanders shall consult with their judge advocates and refer to applicable DOD and Service directives, including DODD 3025.1, *Military Support to Civil Authorities (MSCA),* DODD 3025.12, *Military Assistance for Civil Disturbances (MACDIS),* DODD 3025.15, *Military Assistance to Civil Authorities*, and DODD 5525.5, *DOD Cooperation with Civilian Law Enforcement Officials.*

"NO DOUBLE STANDARD POLICY"

It is the policy of the US Government that no double standard shall exist regarding the availability of terrorist threat information and that terrorist threat information be disseminated as widely as possible. Officials of the US Government shall ensure that information that might equally apply to the public is readily available to the public. The Department of Homeland Security (DHS) is responsible for the release of information to the public in the 50 United States, its territories, and possessions. The Department of State (DOS) is responsible for release of terrorist threat information to the public in foreign countries and areas. Threats directed against or affecting the public (in the 50 United States, its territories, and possessions) or US citizens abroad shall be coordinated with the DHS, the DOS, or the appropriate US embassy before release.

Commanders may disseminate terrorist threat information immediately to Department of Defense (DOD) elements and personnel for threats directed solely against the Department of Defense. In foreign countries and areas, the threat information also shall be passed up the chain of command to the lowest level that has direct liaison with the DOS or the appropriate US embassy(ies) (or for noncombatant commander assigned forces, the US defense representative [USDR]). Within the 50 United States, its territories, and possessions, the threat information shall be passed up the chain of command to the lowest level that has direct liaison with the DHS. Except when immediate notice is critical to the security of DOD elements and personnel, the appropriate DOS/US embassy(ies)/DHS should be informed of the threat information before release to DOD elements and personnel. When immediate notice is critical to the security of DOD elements and personnel, commanders may immediately disseminate the information to, and implement appropriate antiterrorism protective measures for, DOD elements and personnel; and as soon as possible, inform the DOS/US embassies or the DHS, as appropriate, through the chain of command.

Commanders also shall inform the DOS/US embassy(ies) or the DHS of any changes to force protection condition (FPCON) levels or the security posture that significantly affects the host nation/US public. When FPCONs are changed based upon received threat information, both the threat information and notice of the changed FPCON shall be passed up the chain of command to the lowest level that has direct liaison with the DOS/US embassy(ies) (or for noncombatant command assigned forces, the USDR) or the DHS. Coordination and cooperation with the DOS/US embassy or the DHS in these cases is NOT a request for concurrence. Rather, it is informing the chief of mission (COM) or Secretary of Homeland Security of the DOD response to a given terrorist threat. Although the COM or Secretary of Homeland Security may not agree with the commander's assessment, the ultimate responsibility for protection of DOD elements and personnel rests with the commanders in the chain of command. In areas outside the purview of the DHS, the DOS

is responsible to determine whether to release the threat information to US citizens abroad and to deal with the sensitivities of the host nation(s). In the areas under the purview of the DHS, the Secretary of Homeland Security is responsible to determine whether to release the threat information to the US public.

SOURCE: DODD 2000.12, *DOD Antiterrorism (AT) Program*

4. Authority for Handling Terrorist Incidents

a. **Commander's Responsibilities Inside the United States, its Territories and Possessions**

(1) Although the FBI has primary LE responsibility for terrorist incidents inside the US (including its possessions and territories) and the DOD Law Enforcement and Counterintelligence Community has a significant role within departmental areas of jurisdiction, commanders remain responsible for maintaining law and order on DOD installations and vessels. The commanders' AT plans should address the use of security personnel to isolate, contain, and neutralize a terrorist incident within the capability of the commander's resources. Terrorist incidents involving attacks on DOD personnel, facilities, or assets are unlawful acts, which trigger the need for three separate but related activities:

(a) Immediate response, containment, and resolution of an incident.

(b) Investigation of an incident for various purposes, to include protection of the crime scene.

(c) Prosecution of the alleged perpetrators.

(2) In the United States, installation and vessel commanders shall provide initial and immediate response to any incident occurring on military installations or vessels to isolate and contain the incident. In the US, the installation or vessel commanders must notify appropriate Federal or state civilian LE authorities as soon as possible and submit a report into the Joint Protection Enterprise Network within 24 hours following a terrorist incident. This includes notifying the DOD Criminal Investigative Task Force regarding acts of terrorism and war crimes. Primary responsibility for investigating many of the most serious crimes on US Government (USG) property shall normally rest with the DOJ.

For further information regarding use of force by DOD personnel, refer to DODD 5210.56, Use of Deadly Force and the Carrying of Firearms by DOD Personnel Engaged in Law Enforcement and Security Duties; *and CJCSI 3121.01B,* Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces.

(3) DOD may, under appropriate circumstances, provide support to state and/or Federal LE agencies in response to civil disturbances or terrorist incidents occurring outside DOD

installations or vessels. Relevant regulations include DODD 3025.12, *Military Assistance for Civil Disturbance (MACDIS)*, DODD 3025.15, *Military Assistance to Civil Authorities*, DODD 5525.5, *DOD Cooperation with Civilian Law Enforcement Officials*, and DODD 5525.7, *Implementation of the Memorandum of Understanding Between the Department of Justice and the Department of Defense Relating to the Investigation and Prosecution of Certain Crimes*.

(4) In the event the FBI assumes jurisdiction, the Attorney General shall be the Primary Federal Agency for the purpose of concluding the incident. If the FBI declines jurisdiction, the senior military commander will take action to resolve the incident. If requested under pertinent statutes, the Attorney General may request SecDef approval for DOD commanders to provide support to the FBI. Military personnel, however, shall always remain under the C2 of the military chain of command. If military forces are employed during a tactical response to a terrorist incident, the military commander retains command responsibility of those forces. Command relationships should be addressed as part of the request for assistance.

(5) Attacks on DOD personnel or assets within the United States, its territories and possessions outside DOD facilities or vessels are to be contained and resolved by state and Federal LE. Limited exceptions to this rule may occur when incidents involve DOD units outside a DOD installation or vessel and immediate action is necessary to protect DOD personnel and property from immediate threat of injury before local LE or the FBI can respond.

b. **Commander's Responsibilities Outside the United States, its Territories and Possessions**

(1) At overseas locations, just as in the CONUS, DOD commanders have the inherent authority and obligation to defend their units and other US units in the vicinity from terrorist incidents wherever they occur, with the additional requirement to notify the cognizant geographic combatant commander for further reporting to the DOS. DOS notification is made at the geographic combatant commander level for incidents on US facilities or vessels outside the United States, its territories and possessions. The commander is responsible to respond and contain the incident as quickly as possible in order to protect DOD personnel and property from immediate threat of injury. The DOS has the primary responsibility for dealing with terrorism involving Americans abroad. The installation or vessel commander should also implement any provisions of the SOFA or other agreements between the United States and the host government relevant to the incident.

(2) The host government may provide forces to further contain and resolve the incident in accordance with its obligations under international law, the SOFA and other relevant agreements. If the USG asserts a prosecutorial interest, the DOJ shall assume lead agency responsibilities for liaison and coordination with HN LE and prosecutorial agencies.

(3) The inherent right of unit commanders to exercise self-defense in response to a hostile act or demonstrated hostile intent, as reflected in CJCSI 3121.01B, *Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces*, still applies in off-base situations or off-vessel in foreign areas. Unless otherwise directed by a unit commander, military members

may exercise individual self-defense in response to a hostile act or demonstrated hostile intent. If US forces are actually under attack, they retain the inherent right to respond with proportionate, necessary force until the threat is neutralized. The host government should take appropriate action to further contain and resolve the incident in accordance with its obligations under international law as well as any applicable SOFA or other international agreement. In situations other than those triggering the inherent right of self-defense, US military assistance, if any, depends on the applicable SOFA and other international agreements. Such assistance shall be coordinated through the US embassy. Unless immediate action is necessary to protect DOD personnel and property from immediate threat of injury, no US military assistance may be provided to assist a host government without direction from DOD, and in coordination with DOS. The degree of the involvement of US military forces depends on the following:

(a) The incident site.

(b) The nature of the incident.

(c) The extent of foreign government involvement.

(d) The overall threat to US interests and security.

(e) The ability of US forces to sustain their capability to perform assigned missions.

c. **MOU and MOA**

(1) The 1986 Diplomatic Security Act directs the Secretary of State (SECSTATE) to assume responsibility for the security of all USG personnel on official duty abroad, except those under the command of geographic or functional combatant commanders and their accompanying dependents. SECSTATE discharges these responsibilities through the COMs. In December 1997, SecDef and SECSTATE signed the MOU on Security of DOD Elements and Personnel in Foreign Areas (also known as the "Universal MOU"). The MOU is based on the principle of assigning security responsibility to the party — combatant commander or COM — in the "best position" to provide security for DOD elements and personnel. The MOU requires delineation of security responsibilities through country specific MOAs.

(2) Once security responsibility has been agreed upon through the Universal MOU/MOA process, the COM and/or combatant commander (and designated AT planning and response elements) enter into MOA/MOUs with local, state, and/or Federal agencies (domestic) or HN (foreign). These MOA/MOUs augment the installation's organic capabilities and/or are activated when a situation exceeds the installation's inherent capabilities, fulfilling surge requirements needed to respond to a terrorist incident. Therefore, each installation must plan for the worst-case scenario, by planning its response based on its organic resources and available local support through MOA/MOUs. These MOA/MOUs must be a coordinated effort between the many AT planning and response elements of the installation.

(3) Installation specific MOA/MOUs and other special arrangements improve the resources and/or forces available to support any AT plan. These MOA/MOUs may include, but are not limited to, HN and US military police forces, fire and emergency services, medical, Federal/state and local agencies, special operations forces, engineers, detection (CBRNE), decontamination or smoke units, and explosive ordnance disposal (EOD).

d. **AT plans will**

(1) Be implemented by combatant commands, subunified commands, JTFs, component commands, and DOD agencies in accordance with responsibilities and procedures established in DODD 2000.12, *DOD Antiterrorism (AT) Program*, DODI 2000.16, *DOD Antiterrorism Standards*, and DOD O-2000.12H, *DOD Antiterrorism Handbook*.

(2) Be coordinated and approved by the appropriate commander or a designated representative.

(3) Address the use of installation security personnel, other military forces, and HN resources. (In many situations through agreement with HN authorities, the plan will probably evolve into the installation having responsibility "inside the wire or installation perimeter" and the HN having responsibility "outside the wire or installation perimeter." The wide dispersal of work areas, housing, support [medical, child care, exchange, morale, welfare, and recreation], and utility nodes [power grids, water plants] may require US responsibility for certain fixed-site security outside the wire. This could be accomplished by a quick reaction force).

(4) Be coordinated by the combatant commander with both HN and DOS officials.

(5) Be exercised annually with HN resources to ensure that the plan remains appropriate.

e. Although the installation commander may not have security responsibility "outside the wire," he still maintains a security interest. The installation commander must include exterior terrain, avenues of approach, threat capabilities (possession of stand-off weapons such as MANPADS or mortars), hazardous material storage in proximity to the US forces, and HN security processes when developing security plans for the installation, regardless of who provides exterior defense.

5. United States Coast Guard

a. The Commandant of the USCG reports directly to the Secretary of Homeland Security. Under DHS, the USCG maintains its statutory status as one of the five Armed Forces of the United States and conducts national security missions as a Military Service at all times. Upon declaration of war by the Congress **or** when the President so directs (may be via the convenience of any EO) at any time, the USCG may be transferred to the Department of the Navy, consistent with USC. As Service Chief, the Commandant would report directly to the Secretary of the Navy. Importantly, all LE authorities of the USCG would transfer to the Secretary of the Navy, a civilian official. In addition, *posse comitatus* still would not apply to the USCG. MOA with

DOD exist for USCG support of maritime HD and the employment of USCG capabilities and resources anywhere in the world in support of the National Military Strategy.

b. The USCG is the lead or primary agency for maritime HS. As such, the Coast Guard is simultaneously and at all times both an Armed Force of the United States (14 USC 1), and a law enforcement agency (14 USC 89). The Coast Guard's HS mission is to protect the US maritime domain and the US Marine Transportation System and deny their use and exploitation by terrorists as a means for attacks on US territory, population, and critical infrastructure. Additionally, the USCG will prepare for and, in the event of attack, conduct emergency response operations. And, when directed, as the supported or supporting commander, the Coast Guard will conduct military HD operations in its traditional role as a Military Service.

Intentionally Blank

CHAPTER V
ANTITERRORISM PROGRAM: INSTALLATION, BASE, SHIP, UNIT, AND PORT

"Night and day we chased an enemy who never awaited our approach but to harm us, was never found sleeping. Each tree, each hole, each piece of rock hid from our unseeing eyes a cowardly assassin, who, if undiscovered, came to pierce our breasts; but who fled or begged for mercy if we found him face to face."

Unknown Creole during the Haitian War for Independence, 1793

1. Overview of Program Concept

In order to meet the terrorist threat, an integrated and comprehensive AT program must be developed and implemented at every echelon of command. The program applies a wartime defensive mindset to foster a protective posture at all times. AT programs are an integral part of CbT and FP and should be coordinated with DODD 3020.40, *Defense Critical Infrastructure Program (DCIP)*, planning, coordination, community cooperation, and synchronization, which is required for every Service, installation, base, ship, unit, and port.

a. **Command and Control.** When terrorists attack DOD property or personnel, the National Military Command Center becomes the operations center for the Joint Staff and the SecDef. The incident command, control, and reporting responsibilities for terrorist attacks on DOD property or personnel belong to the geographic combatant commander within whose AOR the attack has occurred. For assets under the control of a functional combatant commander (e.g., Commander, United States Special Operations Command) the functional combatant commander will coordinate with the affected geographic combatant commander for an appropriate division of responsibilities. Combatant command reporting will use the National Military Command System.

b. **AT Program Elements.** The AT program stresses deterrence of terrorist incidents through preventive measures common to all combatant commands and Services. In order to be successful, an AT program must be implemented in a methodical, coordinated manner. It cannot be stressed enough that the AT program is the ultimate responsibility of the commander or, in the case of a DOD agency, the civilian equivalent, who has the authority and responsibility to alter or add to the AT program as deemed necessary to accommodate the local situation. The minimum AT program elements include risk management, planning, training and exercises, resource generation, and program reviews. Plans for CM and response are important adjuncts to an effective AT program.

DODI 2000.16, DOD Antiterrorism Standards, *provides the specific requirements for these elements. Similarly, DOD O-2000.12H,* DOD Antiterrorism Handbook*, provides discussion of program elements.*

(1) Risk management is the process of systematically identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk costs

with mission benefits. The commander must decide how best to employ given resources and AT measures to deter, mitigate, and prepare for a terrorist incident while continuing the mission. Risk management has three key sub elements:

(a) Criticality assessment.

(b) Threat assessment.

(c) Vulnerability assessment.

(2) Planning: The AT plan is tailored to the level of command and activity for which established and contains all the measures taken to establish and maintain an AT program that meets the standards of DODD 2000.12, *DOD Antiterrorism (AT) Program*, and DODI 2000.16, *DOD Antiterrorism Standards*. Specific elements of the plan are discussed below and must be integrated into or referenced by the AT plan.

(a) Risk mitigation measures to establish a local baseline or defense posture.

(b) Physical security measures.

(c) Measures for off installation facilities, housing, and activities.

(d) Measures for HRP.

(e) Construction and building considerations.

(f) Measures for logistics and other contracting.

(g) Measures for critical asset security.

(h) Measures for in-transit movements.

(i) Incident response measures.

(j) Consequence management measures, to include CBRNE response planning.

(k) FPCON implementation measures, including site-specific AT measures.

(3) Training and Exercises have the following sub elements:

(a) Annual exercise of AT plans.

(b) Exercise documentation and process improvement/review.

(c) Formal AT training (Levels I-IV for appropriate personnel).

(d) AOR specific training.

(e) Training for HRP and personal security detachment personnel.

(4) AT Resource Generation Requirements include the following:

(a) Use of PPBE process.

(b) CbT-RIF use for emergency requirements.

(c) Unfunded requirements submitted.

(d) Core Vulnerability Assessment Management Program (CVAMP) use.

(5) Program review is required at the following times:

(a) At least annually.

(b) During pre-deployment preparations.

(c) Whenever threat, criticality, or vulnerabilities change significantly.

c. **Key Discussion Topics**

(1) **Criticality Assessment.** The criticality assessment provides the commander with a prioritized list of assets based on the necessity for mission completion (see Appendix A, "Criticality Assessment"). DOD has not yet designated a single criticality process that should be used for all circumstances.

(2) **Threat Assessment.** The terrorism TA is the tool that commanders use to determine the capability, intentions, and activity of terrorist organizations (see Appendix B, "Threat Assessment"). DOD, through the Undersecretary of Defense for Intelligence, has developed a Defense Threat Assessment.

(3) **Vulnerability Assessment.** The VA is the determination of susceptibility to attack by the broad range of terrorist threats (see Appendix C, "Vulnerability Assessment").

(4) **Risk Assessment.** The risk assessment combines the criticality, threat, and vulnerability rating given to each asset and unwanted event. It uses the theory that in order for there to be risk, each one of the elements (Criticality, Threat, and Vulnerability) must be present therefore Risk = Criticality x Threat x Vulnerability. Risk is based on the value of the asset in relation to the threats and vulnerabilities associated with it. Risk is derived by combining the relative impact of any loss or damage to an asset (Criticality) with the relative probability of an unwanted event (Threat x Vulnerability) (see Appendix D, "Risk Assessment").

(5) **Physical Security.** Physical security measures assimilate facilities, equipment, trained personnel, and procedures into a comprehensive effort designed to provide optimal AT protection to personnel and assets. The objective is to ensure an integrated approach to terrorist threats. Well-designed AT measures direct actions that ensure threat detection, assessment, delay, denial, and notification. AT measures should include provisions for the use of physical structures, physical security equipment, CBRNE detection and protection equipment, random antiterrorism measures (RAMs), response forces, and other emergency measures (see Appendix H, "Force Protection Condition System"). AT measures should be scalable and proportional to increases in the local threat and/or unit operational capability.

(6) **FPCON Measures.** FPCON measures are the actions taken at facilities to deter and/or prevent a terrorist(s) from conducting an attack. FPCONs are the principal means through which commanders (or DOD civilian equivalent) apply an operational decision to best protect personnel or assets from terrorist attack (see Figure V-1). The FPCON system is similar to the Homeland Security Advisory System (HSAS) but based on different criteria and designed for different audiences. There is no direct correlation between the HSAS and FPCON system but knowledge of the HSAS may be beneficial during coordination with civilian officials in the US. A conceptual comparison of the two systems is provided in Appendix M, "Homeland Security Advisory System."

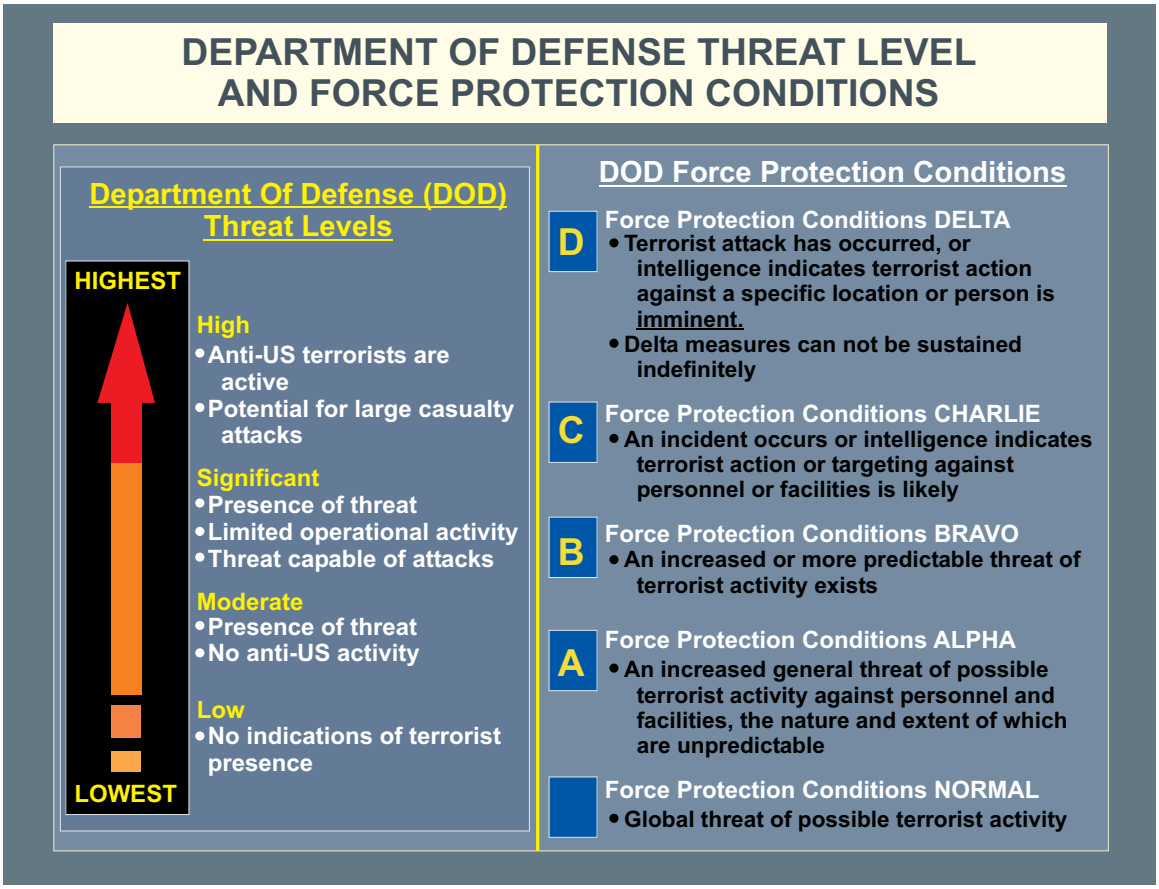


Figure V-1. Department of Defense Threat Level and Force Protection Conditions

(7) **Terrorist Incident Response Measures.** These include procedures to provide command, control, communication, and intelligence to the first responders charged with the task of determining the full nature and scope of the incident, containing damage, and countering the terrorist(s) that may still be present. The term "first responders" refers to local and nongovernmental police, fire, and emergency personnel who in the early stages of an incident are responsible for the protection and preservation of life, property, evidence, and the environment, as well as emergency management, public health, clinical care, public works, and other skilled support personnel (such as equipment operators) who provide immediate support services during prevention, response, and recovery operations. First responders may include personnel from Federal, state, local, tribal, or nongovernmental organizations. The objective of terrorist incident response measures is to limit the effects and the number of casualties resulting from a terrorist attack. These measures and the strategy that ties them together can also contribute to deterring terrorist attacks if our adversaries recognize our ability to mitigate the effects of their attacks.

(8) **Terrorist Consequence Management Preplanned Responses.** Terrorist CM preplanned responses should include emergency response and disaster planning and/or preparedness to recover from a terrorist attack, to include WMD. Although not elements of AT, plans for CM preparedness and incident response measures as well as plans for continuing essential military operations are important adjuncts to an effective AT program. In addition, special circumstances imposed by terrorist attacks utilizing WMD shall require immediate close coordination with higher command and HN, and/or Federal, state, and local authorities, and may require CBRNE subject matter expertise assistance or support from Defense Threat Reduction Agency (DTRA) or other sources.

(9) **Coverage for Off-Base Assets.** In planning the coverage of off-base assets and infrastructure selected for inclusion in the facility, installation, or activity AT program, include notifications to the appropriate first responders, including LE offices, and the servicing FBI field office. This shall enable integration of the facility into their response and contingency planning and provide a potential source to assist the facility in its own preparations and response. As necessary, validate and monitor the scope and viability of the coverage. If the asset is a cleared contractor facility, provide for reporting to the servicing Defense Security Service (DSS) Industrial Security Field Office (see DOD 5520.22-R, *Industrial Security Regulation*) of information that indicates classified information under facility control is or could be at risk. Promptly notify the servicing DSS office of any security requirements which the installation or activity intends that the cleared industrial facility implement.

2. Antiterrorism Plan Development

a. The commander is responsible for the development of the AT plan. The antiterrorism officer (ATO) is normally assigned the task of actually writing the plan. The ATO should leverage the capabilities of the organization's AT working group (ATWG) to assist in the process. Using the ATWG ensures the participation, input, and "buy-in" of the necessary subject matter experts and others with key responsibilities.

b. Everyone involved in developing the plan must be familiar with all applicable AT directives and instructions. Use of the JAT Guide, available from the Joint Staff J-3 Deputy Directorate for Antiterrorism and Homeland Defense and at www.atep.smil.mil, will facilitate preparation of the AT plan for installations, in-transit, and expeditionary locations. AT plans are not usually considered valid until they have been signed by the responsible commander, exercised and tested.

3. Combatant Commander's Responsibility

The combatant commander designates a staff officer, usually in the HQ, operations, LE, or security element, to supervise, inspect, test, and report on AT programs within the command. This staff officer also coordinates with Federal, local, state, or HN authorities and US embassies and consulates. Simultaneously, the J-2 disseminates intelligence on terrorist activities to subordinate and supporting commands to ensure that the AT measures are appropriate to the threat. The manner in which the combatant commander places importance on these staff functions usually has a direct effect on the AT readiness of subordinate commands.

CHAPTER VI
PREVENTIVE MEASURES AND CONSIDERATIONS

"A general should direct his whole attention to the tranquility of his cantonments, in order that the soldier may be relieved from all anxiety, and repose in security from his fatigues."

Attributed to Frederick the Great

1. Commander's Responsibility to Manage Terrorism Risk

a. Although the risk of terrorist aggression against US and multinational resources cannot be totally eliminated, it can be reduced and managed through deliberate and effective risk management. Command planning and execution should include actions to implement AT measures which are consistent with fundamental risk management principles. Through the application of basic risk management principles of identification, assessment, risk avoidance, loss prevention, loss reduction, and process evaluation/reapplication, most FP requirements can be met.

b. Preventive and protective security measures should be taken by military units and individual Service members to protect themselves and their ability to accomplish their mission during mobilization, deployment, employment, sustainment, and redeployment operations. Additionally, rest and recuperation (R&R) facilities and other facilities not located in a traditional military installation also require close consideration. These facilities are frequently vulnerable due to their location and generally easy access. Service personnel are at risk of lowering their guard while using these R&R facilities. The installation, ship, unit, or port AT plan provides the mechanism to ensure readiness against terrorist attacks while the unit performs its tactical mission during deployments. Air shows, or similar events, should receive special consideration and be covered under specific AT plans or contingencies. The ATO should review special events and prepare recommendations or specific AT supplemental plans for the installation commander. The degree of the protection required depends on the threat in a given location. Commanders must constantly evaluate security against the terrorist threat in order to effectively evaluate security requirements. This responsibility cannot be ignored.

2. Antiterrorism Measures

The following AT TTP include actions for both conventional installations or locations and higher threat areas. Commanders should review individual measures based on threat, vulnerabilities, criticality, and risk assessments as discussed elsewhere in this publication.

a. **Installations, Ships, and Expeditionary Sites.** Forces are frequently employed for security operations or other short-term, conventional, combat-related tasks. Easily defended locations are often rare in urban areas because of building and population density or lack of proper cover and concealment and an inability to create perimeter stand-off. Political restrictions may also limit the military's ability to construct fortifications or disrupt areas. Commanders, however, must take all practical means to ensure FP and identify shortcomings to appropriate

levels of command for resolution. Military planners should adapt existing structures to provide protection based on the mission, potential for attack, and ability to use surroundings effectively.

(1) **Estimate of the Situation.** The commander and staff should complete a thorough estimate of the situation using mission, enemy, terrain, troops, time, and political planning factors in developing a security assessment. Figure VI-1 aids in developing an estimate of the terrorist situation.

(2) **Develop Plan.** Planning should include a combination of LE and security assets such as barriers, sensor employment, other obstacles (such as ditches or barriers) (see Figure VI-2), local-hire security personnel (if applicable), unit guards, deception, and on-call support from reaction forces. Each situation requires its own combination of abilities based on available

SITUATION ESTIMATE CHECKLIST	
MISSION	Who is being tasked? What is the task? When and where is this task to take place? Why are we performing this task?
ENEMY	Who are the potential terrorists? What is known about the terrorists? What is their agenda, capabilities? Where is their support infrastructure? Are they supported by the local population? How can they be recognized? How do the terrorists receive information? Have they infiltrated the installation, port, host-nation military or the local law enforcement? How might the terrorists attack? What are the potential weapons and tactics a terrorist organization could employ, these include snipers, mortars, rockets, air or ground attacks, suicide attacks, arson, or kidnappings? (Note: Use of the threat matrix identified in Chapter 5 of Department of Defense O-2000.12H will aid in identifying weapons and tactics.) Does your unit have routines? What is the potential for civil disturbances and could terrorists use or influence these disturbances in an attack? Local law enforcement personnel and host and friendly nation intelligence services can be valuable sources of information.
TERRAIN	What are the strengths and weaknesses of the installation, base, ship, port, and local surroundings? Are the avenues of approach above or below the water or ground? Are there observation areas, dead spaces, fields of fire, illumination, or no-fire areas (e.g., schools)? Are there tall buildings, water towers, or terrain either exterior or adjacent to the perimeter that could become critical? What toxic industrial materials (chemical, biological, radiological, nuclear) are stored in or transit your area?

Figure VI-1. Situation Estimate Checklist

SITUATION ESTIMATE CHECKLIST (cont'd)	
TROOPS	Are other US forces or equipment available? What local law enforcement, host nation, allied or friendly nation assets might be available? How do I vet non-US personnel, such as contractors and other foreign or third country nationals who come on to the base? Are engineers and/or explosive ordnance disposal in the area and will they be able to provide support? Are emergency reinforcements available? Are military working dog teams available? What are the host-nation responsibilities, capabilities, and attitudes toward providing assistance? What restraints will be imposed by the US Government on the show or use of force?
COMMUNICATIONS	Is there a method for mass alerting across the base? What radios are used on base? Are they secure? Is there redundancy in the system?
TIME	What is the duration of the mission? Are there time constraints? Will there be sufficient time to construct force protection facilities such as barriers, fences, and lights?
POLITICAL PLANNING FACTORS	Are there host-nation concerns or attitudes that will impact on the situation? Will the situation be influenced by the existence of any religious, cultural, racial, or allied political concerns?

Figure VI-1. Situation Estimate Checklist (cont'd)

resources and perceived need. Incident response and CM planning should include considerations for fire response, CBRNE and toxic industrial material (TIM) response (including in place sheltering and evacuation considerations), mass notification, EOD/IED response, medical response and evacuation, and mass casualty procedures.

(a) **Obstacles.** Obstacles slow down or disrupt vehicles and personnel approaching an area. Constructing vehicle barriers by using commercially installed electronic barriers, trenches, masonry barriers, concrete-filled oil drums, or vehicles staggered across the route creating a zigzag maze forces vehicles to slow down and make sharp turns and exposes the driver to capture or direct fire. Scattering speed bumps or sandbags on the route further slows traffic. Also consider employment of road spikes, dragon teeth, or tire shredders to slow down unauthorized traffic. The force protection equipment demonstration usually produces a compilation of useful equipment and can be found online or requested from DTRA at atfphelp@dtra.mil. Designing entrance gates to allow access to authorized personnel while denying access to unauthorized personnel by use of controlled turnstiles provides time for observation and protection to guards and slows down direct frontal attacks. Fences, entrance gates, and obstacles should be illuminated to provide easy observation. Obstacles must be covered by observation and fire. Figure VI-3 shows a notional entry control point (ECP). Although

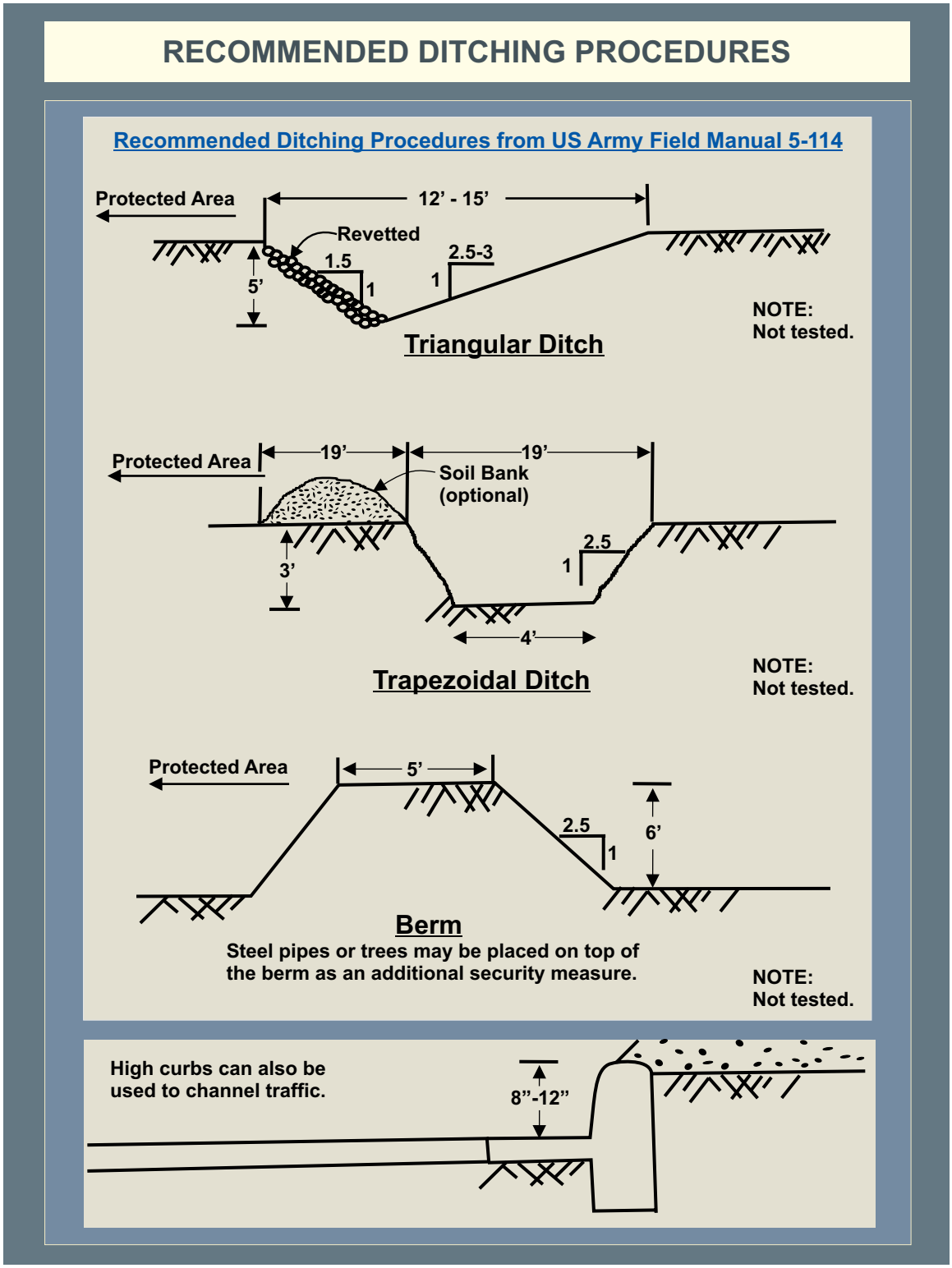


Figure VI-2. Recommended Ditching Procedures

individual ECPs will not be identical to this design because of terrain, location, personnel availability, etc., this design shows several key design elements, including truck inspection lane, pedestrian lane, turn around area, overwatch and other control features. In essence, ECP design

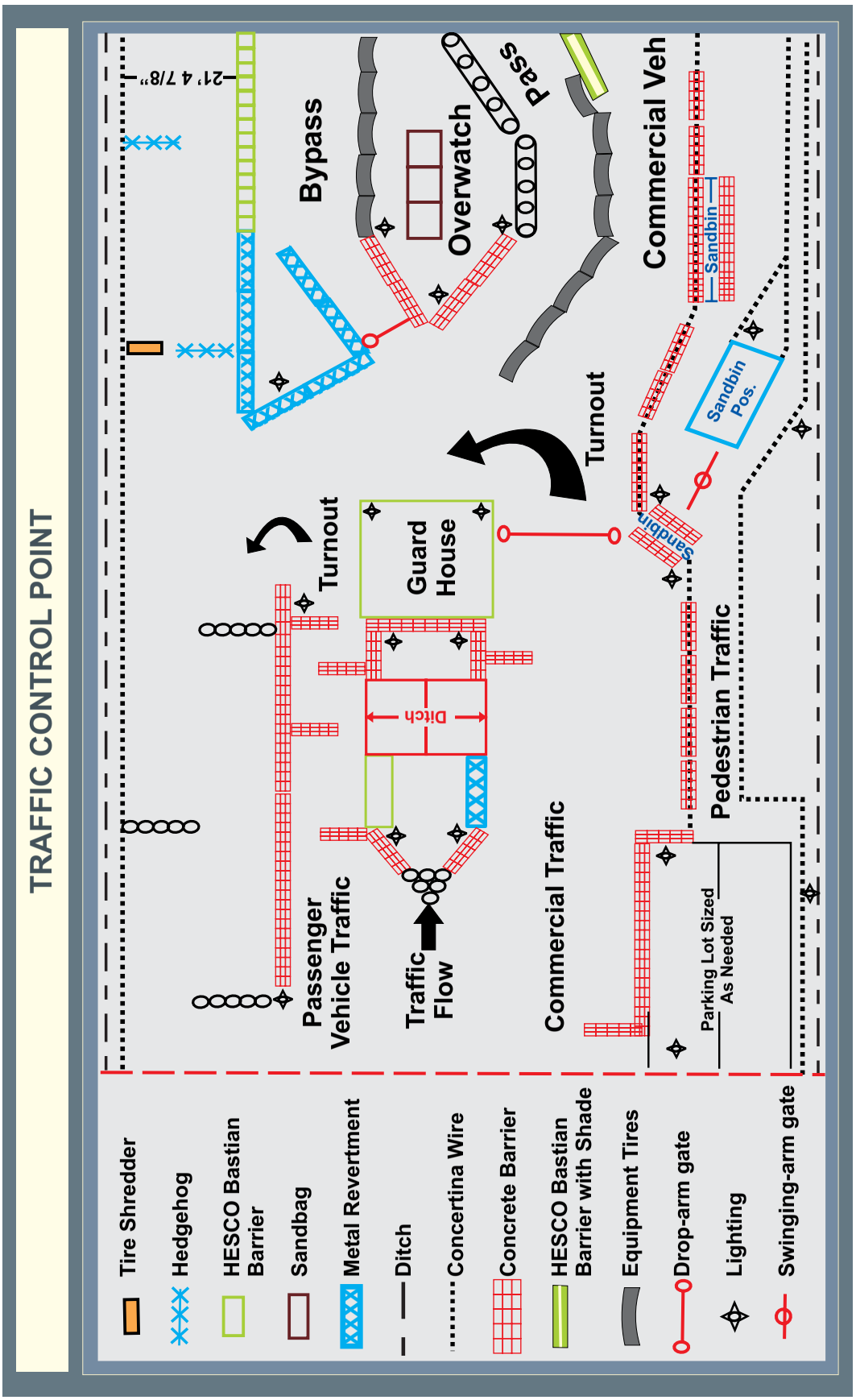


Figure VI-3. Traffic Control Point

should consider four zones: an approach zone where traffic speed and maneuver is limited and vehicle type (passenger, friendly, commercial) is established; the access control zone where personnel and vehicle credentials are established and vehicle inspections occur (this area should be screened to protect from surveillance by enemy forces); the response zone, which provides adequate reaction time for ECP personnel; and a final denial barrier that requires positive action to allow entry or exit from a compound.

(b) **Local Security.** Local security must be around-the-clock to provide observation, early warning and, if necessary, live fire capabilities. The security should include guards at entrances to check right of entry in observation posts (OPs), around perimeter, and on rooftops to view the surrounding area. These guard positions must also be integrated into the AT plan to enable their use in augmenting responding LE personnel. Security personnel should have available to them and be trained in specialized equipment for responding to terrorist attacks and/or incidents (see Figure VI-4). Local installations, with the assistance of the parent Service, should identify and procure this equipment based on Service directives and the local situation. Security review should also include review of procurement, storage, and preparation of food supplies used on base. A food vulnerability assessment can be initiated by food services personnel to review the complete food process.

Figure VI-4. Security Force Equipment

(3) **Establish Defense.** Measures taken to establish the defense must be continually reviewed and progressively updated to counter the changing threat and add an element of unpredictability to the terrorist's calculation. Defensive measures include the following:

(a) Determine priority of work (assign sectors of observation and fire, construct obstacles, fortify).

(b) Improve obstacles, fortifications, and the defense as a whole. Long-term deployments should program engineer assets and FP or physical security funds toward the construction of permanent fixtures.

(c) Establish inspections and immediate action drills, exercises, and training to implement the security plan.

(d) Maintain, when possible, secure radio or landline communications with the military police, security guards, and reaction force(s).

(e) Keep abreast of current military and HN police and intelligence assessments.

b. **Guard Duties.** Guard duties are detailed in general and special orders and standard operating procedures. Special orders should address as a minimum the following:

(1) Details of authorized passes; provide samples of passes.

(2) Procedures for searching people and vehicles.

(3) Response to approach by unauthorized personnel or hostile crowds.

(4) Specific ROE or use of force policy.

(5) Response to unauthorized photography and surveillance activities.

(6) Steps necessary to obtain police, reaction force(s), fire department, and ambulance.

(7) Guidelines for contact with HN police.

(8) Guidelines for contact with press and media.

(9) Evacuation procedures.

c. **Road Movement.** Road movements are always vulnerable to terrorist attacks in high-risk areas. Road reconnaissance should be conducted periodically to identify high-threat areas. If possible, alternate forms of transportation (e.g., helicopters) should be used. If road movement is required:

(1) Avoid establishing a regular pattern.

(2) Vary routes and timing.

(3) Travel in groups, never single vehicles.

(4) Do not stop for dead or dying animals in/beside the road.

(5) Do not allow people to walk-up to vehicles.

(6) Avoid traveling at night unless tactical advantage can be gained through use of night vision devices. Additional precautions should be considered if travel is required during periods of agitation (e.g., religious or political holidays).

(7) When possible, keep a low profile (use vehicles that do not stand out).

(8) Plan alternate routes and reactions to various threatening scenarios.

(9) Plan communications requirements.

(10) Avoid dangerous areas (e.g., ambush sites, areas known for violence).

(11) Provide adequate security.

(12) Plan in advance for maintenance and evacuation.

(13) Use countersurveillance.

d. **Vehicle Protection.** Consider the following precautions when using tactical and some types of commercial vehicles, such as trucks, in a high-risk area:

(1) Place sandbags on floorboards and fenders.

(2) Cover sandbags with rubber or fiber mats.

(3) If carrying personnel, sandbag the vehicle bed as well as the driver's compartment.

(4) Remove canvas so passengers can see and shoot.

(5) Fold windshield in driver's compartment and fit high-wire cutter. Lower side windows (unless windows provide ballistic protection) to prepare to use weapon through window.

(6) Normally, avoid large concentrations of personnel in any one vehicle. If necessary, assign convoys additional vehicles to disperse personnel loads.

(7) Passengers riding in truck bed face outboard and are assigned sectors of observation and fire.

(8) Rig chicken wire or chain link screens on front bumper frame to deflect rocks, bottles, firebombs, and grenades.

(9) Carry pioneer tools (fire extinguishers in particular), a line with grappling hook to clear obstacles, and tow bars for disabled vehicles.

(10) When the threat of hostile fire is constant, plan for the use of vehicles with additional armored protection.

e. **Convoys.** In extremely high-risk areas, consider using armed escorts for convoy protection.

(1) Develop and rehearse immediate action drills before movement.

(2) Perform route clearance before movement.

(3) Establish and maintain communications throughout the route.

(4) Develop deception plans to conceal or change movement timing and route.

(5) If possible, include HN police and/or military personnel in the convoy.

(6) When selecting routes, avoid entering or remaining in dangerous areas. If ambushed, gauge response by enemy strength. Counter ambushes by accelerating through the ambush area, counterattacking, withdrawing, or withdrawing and staging a deliberate attack.

(7) Convoy escort composition depends on available forces. Vehicles used should be appropriately hardened and possess the necessary weapons systems and other equipment to address the threat. Helicopter and AC-130 gunships can also be used as air escorts, if available. Escorts should be organized into an advance guard, main body escort, and reaction or strike group. Planning considerations are as follows:

(a) Determine concept of operation.

(b) Identify available transportation.

(c) Identify order of march and road organization.

(d) Identify disposition of advance guard, main body escort, and reaction or strike group.

(e) Designate assembly area for convoy.

(f) Determine rendezvous time at assembly area, departure time of first and last vehicle, and expected arrival of first and last vehicle at destination.

(g) Identify action upon arrival.

(h) Determine required coordinating instructions for speed, spacing, halts, immediate action drills, breakdowns, and lost vehicles.

f. **Rail Movement.** Rail movement is the most difficult form of transportation to conceal and protect because it follows a predictable route and rail heads are difficult to conceal. Opportunities for deception are limited and physical security is critical. The following security precautions should be considered:

(1) Restrict passengers to military personnel only.

(2) Search for explosives or possible hijackers before departure and after every halt (military working dogs [MWDs] are particularly suited for this mission).

(3) Ensure that the railway is free of obstructions or explosives.

(4) Patrol the railway area.

(5) Place armed security personnel on duty throughout the train, including engine room and trail car.

(6) Patrol and guard departure and arrival stations.

(7) Use deception measures.

(8) Provide air cover (e.g., AC-130, helicopter gun ships).

(9) Maintain communications within the train and with outside agencies.

(10) Provide reaction force to be moved by air or coordinate host-nation support (HNS) (if available).

g. **Sea Movement.** Sea movement, especially aboard military vessels, may provide a false sense of security. Sea operations are certainly more secure than urban patrols; however, ships transiting through restricted waterways such as straits, harbors, or anchored off hostile coastlines are visible and high-risk targets. Crews of ships in harbors need to evaluate each new port and determine possible terrorist actions and ship's force counteractions (such as using fire and steam hoses to repel attackers). Crew members must be aware of HNS and responsibilities while in

port or anchored in foreign national waters. The ship's captain is solely responsible for the ship and all those embarked. As a minimum, the captain:

(1) Establishes methods of embarkation and debarkation and patrol activities for all personnel.

(2) Identifies vital areas of the ship (for example, engine room, weapons storage, command and control bridge), and assigns security guards.

(3) Coordinates above and below waterline responsibilities.

(4) Establishes a weapons and ammunition policy i.e., ROE, and appoints a reaction force (e.g., ships self-defense force, pickets, and security teams).

(5) Ensures all personnel involved are trained through exercises or drills.

h. **Air Movement.** For the most part, while a unit is being transported by air it is under the purview of the Air Force or air movement control personnel. Troop commanders and Air Force personnel coordinate duties and responsibilities for their mutual defense. Personnel must remain vigilant and leaders must provide adequate security. Unit security personnel coordinate with airfield security personnel, assist departures and arrivals at airfields while en route, and determine weapons and ammunition policies. Special considerations include the following topics:

(1) Road transport security when driving to and from airfields is critical. Keep arrival arrangements low profile. Do not pre-position road transport at the airport for extended periods before arrival.

(2) If pre-positioned transport is required, attach a security element and station it within the airfield perimeter. Security at the arrival airfield can be the responsibility of the HN and requires close coordination. Maintain communications between all elements until the aircraft is "wheels-up" and, upon arrival, reestablish communications with the new security element.

(3) All personnel (air crews and transported unit) must be cautioned concerning the transportation of souvenirs and other personal items that could be containers for explosives.

(4) Man-portable weapons systems in the hands of terrorists create additional planning challenges for the security of aircraft. Planning considerations should include defensive measures against such systems in the choosing of airfields and forward arming and refueling points.

i. **Patrolling.** Units outside the United States may be called upon to conduct patrols in urban or rural environments. These patrols will normally be planned and executed in conjunction with HN authorities and should be coordinated with the representatives of the appropriate staff judge advocate (SJA) office and be in accordance with any applicable basing, status-of-forces, or other agreements. Patrols support police operations, expand the area of influence, gather information, police nightclubs and restaurants, detain individuals as required, conduct hasty

A coalition QRF prepares to move.

searches, and erect hasty roadblocks. Patrols must understand the ROE. Patrolling units should avoid patterns by varying times and routes, using different exit and entry points at the base, doubling back on a route, and using vehicles to drop off and collect patrols and change areas. Base sentries or guards, other vehicle patrols, helicopters, OPs, HN assets, and reaction forces provide additional support.

j. **Roadblocks.** There are two types of roadblocks: deliberate and hasty. Deliberate roadblocks are permanent or semipermanent roadblocks used on borders, outskirts of cities, or the edge of controlled areas. Use deliberate roadblocks to check identification and as a deterrent. Use hasty roadblocks to spot check, with or without prior intelligence. Hasty roadblocks use the element of surprise. Their maximum effect is reached within the first half hour of being positioned. Hasty roadblocks can consist of two vehicles placed diagonally across a road, a coil of barbed wire, or other portable obstacles. Roadblocks must not unnecessarily disrupt the travel of innocent civilians. Personnel manning roadblocks must know their jobs thoroughly, be polite and considerate, act quickly and methodically, use the minimum force required for the threat, and promptly relinquish suspects to civil police authorities. General principles considered in establishing roadblocks are concealment, security, construction and layout, manning, equipment, communications, and legal issues. Unless combined posts (HN and US personnel) are used, language training will be a key planning factor in employing roadblocks.

k. **Observation Posts.** OPs are critical. OPs provide prolonged observation of areas, people, or buildings. OPs allow observation of an area for possible terrorist activity (avenues of

approach); observation of a particular building or street; ability to photograph persons or activities; ability to observe activity before, during, or after a security force operation (e.g., house search); and ability to provide covering fire for patrols. Special factors apply to OPs located in urban areas. The OP party and reaction force must know the procedure, ROE, escape routes, emergency withdrawal procedures, rallying point, casualty evacuation, and password. Cover the occupation and withdrawal of an OP by conducting normal operations (e.g., house searches, roadblocks, patrols to leave people behind), flooding an area with patrols to disguise movement, using civilian vehicles and clothes (when authorized), and using deception. Any compromise of an OP location should be immediately reported.

l. **Civil Disturbances.** Crowd violence can either be a spontaneous emotional eruption or a planned event. In the latter case, its purpose is to draw police or troops into a target area or away from some other event. Crowd violence may also involve violence within the crowd or from opposing groups. Crowd violence is characterized by incitement and violence; both are highly contagious. Riot control aims to restore order with minimum use of force. Bearing in mind that the size or motivation of the crowd may prevent its control, the general approach is to reduce or disrupt the crowd's unifying influences and reorient the participants to concerns for personal vulnerability and welfare. The principles of riot control are shown in Figure VI-5.

m. **Bomb Explosion or Discovery.** The initial terrorist bomb may not be the end of the incident. The initial bomb may be designed to draw forces into an area as targets for a shooting

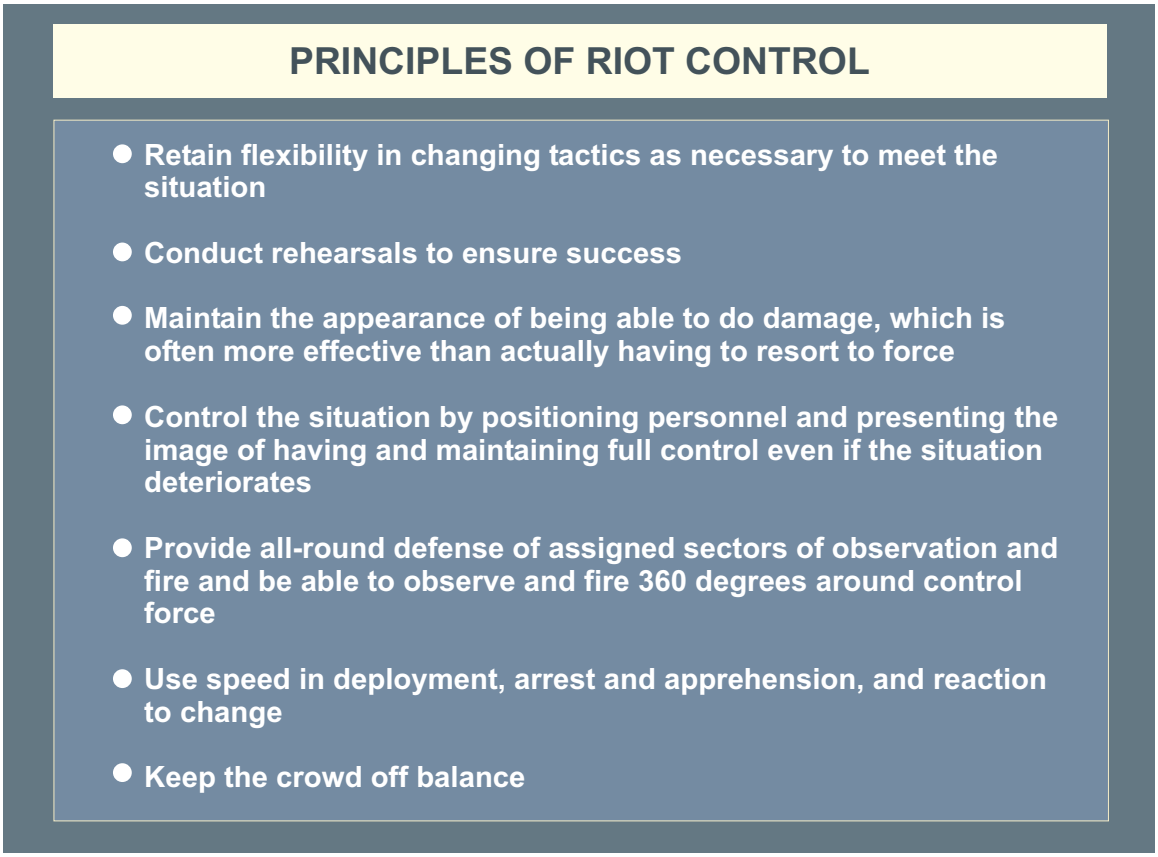


Figure VI-5. Principles of Riot Control

ambush or another explosion. It is imperative to detail personnel or units to search the area for secondary devices. Upon discovery of a bomb or upon entering a bomb site, response forces should proceed with extreme caution and contact the EOD team immediately. Explosive detection MWDs, EOD or other available detection methods should be utilized to sweep areas surrounding suspected explosive devices or incident sites for secondary devices.

n. **Personal Protective Measures.** Overseas deployments require a high degree of personal protective measures. DOD personnel must be aware of basic personal protective measures against terrorism, specific threats for the area they will operate in or transit, and specialized training which their duty or position requires, but the commander must also focus on the exposure of the troops to any special terrorist threat. This requires particular attention to areas where troops will live, work, and conduct R&R. Coordination between military intelligence, CI and LE agencies and HN forces is critical. The deployed military member must also understand the threat and required personal security measures.

3. Design Basis Threat

a. Design basis threat (DBT) is the threat against which an asset must be protected and upon which the protective system's design is based. It is the baseline type and size of threat that buildings or other structures are designed to withstand. The DBT includes the tactics aggressors will use against the asset and the tools, weapons, and explosives employed in these tactics. DBT is defined in Technical Manual (TM) 5-853, *Security Engineering*, and the Military Handbook 1013/12. It is also included in UFC 4-010-01, *DOD Minimum Antiterrorism Standards for Buildings*.

b. The DBT is used by engineering and facilities personnel to protect personnel and mission with proper design. It is important that the "threat used as a basis of design" be a steady state threat and realistic. This value is used as the beginning input to the design loads which the building structure will have to support or withstand during the life of the building.

c. Installations can determine the DBT by identifying the highest threat severity and tactic that they will likely face. Alternatively, they can incorporate the DBT specified by higher HQ. If higher HQ guidance does not provide a DBT, the installation should establish and incorporate a DBT for use by security engineers.

d. The generic design threat of a bomb (equivalent explosive weight in TNT [Trinitrotoluene]) inside the installation perimeter drives facility barrier planning. Determining the minimum standoff from parking and roadways at mission essential vulnerable area (MEVA), high-value targets, or high-density targets requires an engineering assessment of the structural vulnerability of the building components against the design threat explosive blast at the level of protection sought. A MEVA is a facility or asset under the jurisdiction of the commander that, by virtue of its function, is determined by the commander to be vital to the success of the mission. Similar design threat input is needed in the AT plan for moving vehicle attack and ballistics attack. A protective system integrates all the protective measures and procedures required to

protect assets against their DBT. The ideal protective system deters, defends against, and defeats aggressors.

e. The off-base threat along the perimeter is different from the on-base standoff to facilities. Adopt this DBT in vehicle barrier planning, and in new and renovation construction. It is noted that the on-base DBT is applicable only if vehicles are thoroughly inspected (including automobile trunks) at the access control point (ACP). If not, then the off-base threat is applicable on-base for locations such as a vehicle parked next to a building. Continue to be aware of the threat. Shift between on-base threat and off-base threat if the security measures at the ACP change to allow the threat easy access to the installation.

4. Barrier Planning

The current environment is dynamic and terrorism is real, evolving, and continues to increase in frequency and lethality. Vehicle bombs have proven to be a viable method of terrorist attacks. The wide availability of bomb making material, ability to conceal explosives in vehicles, and ease of getting vehicles to a target has made this a successful tactic. Commanders must manage or mitigate the risk of a vehicle bomb attack by hardening facilities or establishing standoff. Standoff, effective and cost efficient, is accomplished by effective facility barriers.

a. The barrier plan represents the interrelationship (interdependency) between threat, required standoff, and wall (window) or structure strength (see Figure VI-6). Similar to all triangles, when one of these parameters changes, the other sides must also change. When any two of these are known, the third can be solved using blast range to effect information.

b. Installations should develop a barrier plan based on DBT and building construction. Use range-to-effect charts to refine the barrier plan so that it will afford the desired level of protection for all MEVAs and critical and primary gathering facilities. Trained Department of Public Works security engineering personnel would also facilitate development of the barrier plan.

c. Barrier plan developers should provide sufficient details in the barrier plan to ensure it can be effectively and efficiently executed. The plan should be refined at least annually to incorporate lessons learned from previous efforts. Barrier plan execution should be resourced to include the time required for barrier placement, and availability of sufficient working heavy equipment. Barriers must block vehicular access to buildings. A diagram showing barrier placement should also represent sufficient passive barriers as outlined in Field Manual (FM) 5114 and TM 5-853-2 at increased FPCONs. Detailed diagrams/maps should show entire building perimeter. Additional barriers may be required. Specific barrier placement and separation should also be included and will greatly facilitate correct plan execution. One note of caution when using water-/sand-filled barriers is to include the time required to fill the barrier, not just moving the barrier to the location.

d. Plans should include sufficient detail to allow efficient and proper positioning of barriers. Maps should show the exact location and spacing of barriers. Physical locations at each facility

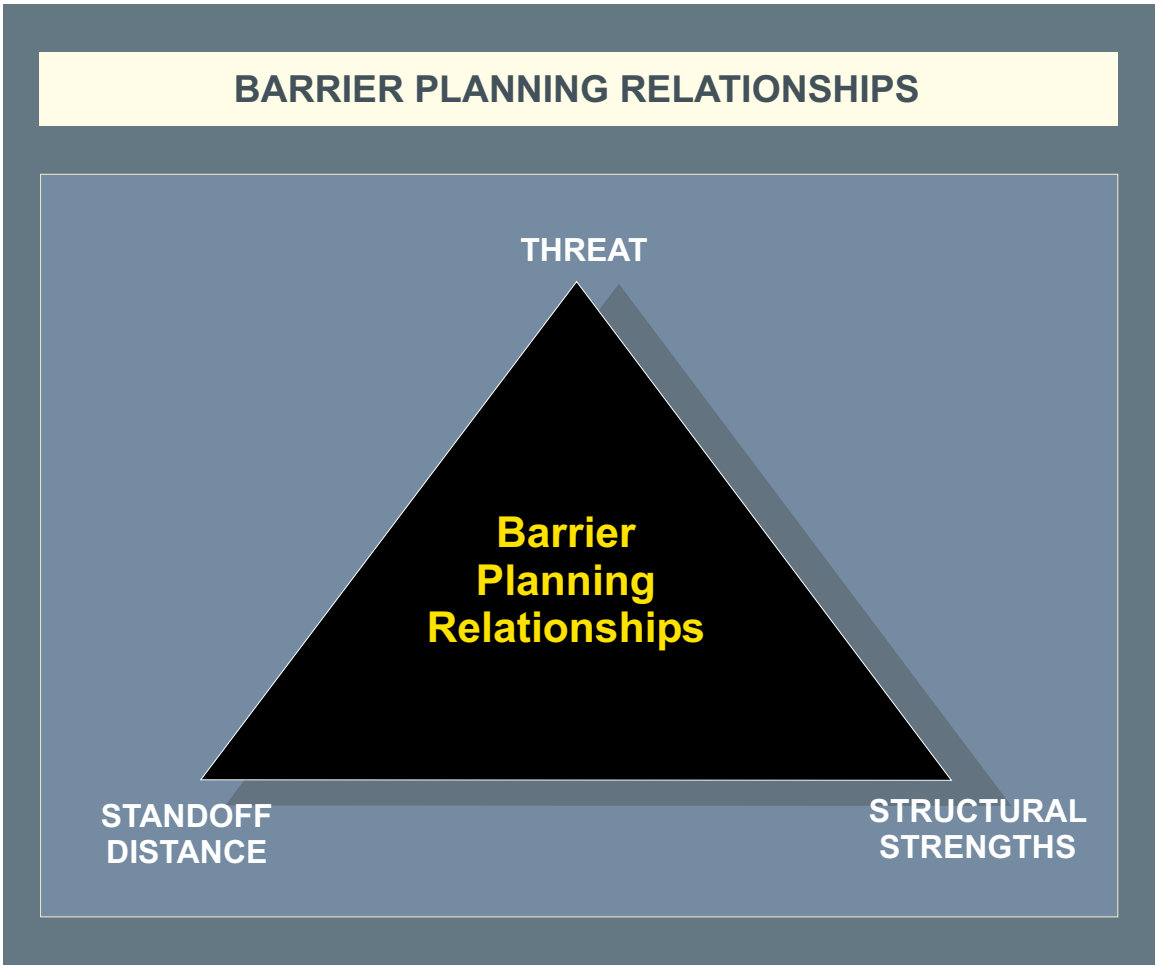


Figure VI-6. Barrier Planning Relationships

can be marked with paint to indicate exact position or ECP and eliminate any confusion. Standoff requirements should increase as threat increases. Therefore, a barrier plan that progresses through each FPCON should be developed. The following considerations should also be included in a facility barrier plan.

(1) **Determine facility to be protected.** Determining the assets to be protected and the level of protection with acceptable risk to assets is the first step in establishing a barrier plan. Facilities with high exposure and high concentrations of personnel should be considered at higher risk. Next, determine the value of the asset by evaluating four factors: mission criticality to the military, mission criticality to the user, replaceability, and relative value. Finally, determine the type of aggressors likely to threaten the asset and the likelihood of attack. Apply this process to all assets on the installation to determine which assets need to be protected with barriers.

(2) **Determine building elements.** Building elements include the layout and the structural design of walls, windows, roofs, and framing systems. Necessary standoff distances can then be determined for each building based on the explosive effects and the desired levels of protection.

(3) **Select standoff zone type(s).** Determination of required standoff is based on operational considerations related to type of building construction and size of explosive threat. Standoff zones must completely surround the facility. Access for entry into standoff zones is through the ECP.

(a) **Exclusive standoff zone.** A controlled area surrounding a facility into which only service and delivery vehicles are allowed. Vehicles must be searched and cleared at an ECP before entry is allowed. ECPs need not be continuously manned if few vehicles are likely to be granted entry. Exclusive standoff zones are usually used for areas closest to vital facilities.

(b) **Nonexclusive standoff zone.** A controlled area used in conjunction with an exclusive standoff zone that provides less restrictive land use than an exclusive standoff zone. Where a nonexclusive standoff zone is employed, it encloses an exclusive standoff zone. Cars (but not trucks) may be granted uncontrolled access to a nonexclusive standoff zone. Trucks must be searched because of the greater capacity to carry explosives. ECPs must be continuously manned while the facility is in operation due to the large number of vehicles likely to be allowed entry (requires additional manpower).

(c) **Facility clustering.** Where there are multiple facilities subject to vehicle bomb threats in the same general area, these facilities may be clustered into common standoff zones to use land and guard manpower more efficiently.

(4) **Determine required standoff distances.** Standoff distances are selected based on building construction (new, existing, expeditionary, and temporary), threat severity levels, and the value and availability of land. If required standoff is not available or achievable, alternate means to mitigate threat (e.g., harden facility, build blast wall) must be evaluated, a decision made to accept additional risk, or restrict use at higher FPCONs.

(5) **Select perimeter barriers.** Perimeter barriers define and maintain the boundaries of the standoff zones. Vehicle barriers are categorized as either active or passive. An active barrier requires some action, either by personnel, equipment, or both, to permit/deny entry of a vehicle. Active barrier systems include retractable bollards, drum type barriers, gates, and active tire shredders. A passive barrier has no moving parts. Passive barrier effectiveness relies on its ability to absorb energy and transmit the energy to its foundation. Jersey barriers, static bollards or posts, ditches, and reinforced fences are examples of passive barriers. Barrier selection is different for either the stationary or moving vehicle bomb tactic and should be based on current TA.

(a) **Moving vehicle bomb tactic.** In this tactic, an aggressor drives an explosive-laden car or truck into a facility and detonates it. The aggressor's goal is to damage or destroy the facility and kill people. This is usually a suicide attack. The specific barrier selected for defending against this tactic must physically stop the kinetic energy (mass times velocity) of a moving threat vehicle at whatever speed it can attain as it approaches the barrier. If the barrier cannot stop that kinetic energy, reduce the speed of vehicle with serpentine and/or speed bumps.

(b) **Stationary vehicle bomb tactic.** In this tactic, an aggressor covertly parks an explosive-laden vehicle near a facility. The aggressor then detonates the explosives either by time delay or remote control. The aggressor's goal is the same as the moving vehicle tactic with the additional goal of destroying additional assets within the blast area. Barriers are not required to provide physical resistance to stop a vehicle for this tactic.

(6) **Identify ECP requirements.** The standoff zone entrance (and exit) is an ECP. Vehicles and personnel are granted authorization to enter the standoff zone and are searched, if necessary, at the ECP. ECP requirements are different for exclusive and nonexclusive standoff zones.

(a) The ECP into an exclusive standoff zone generally requires only a single entry lane because of limited traffic into the zone. It also requires an active barrier to keep vehicles from passing through unhindered. The ECP need not be continuously manned and can be operated remotely if some form of communication between the facility and the ECP exists so that drivers can request entry.

(b) A nonexclusive standoff zone ECP will usually need to be continuously manned and will require some form of shelter for the guard. It also requires active barriers. Determine the number of entry/exit lanes required based on the anticipated peak hourly volume of vehicles that will enter the standoff zone.

(c) If an ECP will be used at night, it will need lighting to support guard searches of vehicles and verification of vehicle and driver identification. Security lighting also acts as a psychological deterrent to potential aggressors. For exclusive standoff zones, the lighting may be turned off except when a guard needs light to process a vehicle.

(7) **Establish standard operating procedures (SOPs).** SOPs explain how active barriers are employed, operated, control access, and outline specific ROE. The ROE should address activating barriers against a threatening vehicle at high speed, which is considered use of deadly force. All security personnel should be alert, well trained, show good judgment, and fully understand current threat, SOP, and ROE.

e. A good barrier plan is well designed, based on a current TA and the commanders acceptance of risk, is operational with AT plans and FPCON system, assigns specific actions and responsibilities for employment, and is represented pictorially. All barrier plans need to be exercised. Consider an initial tabletop exercise of your barrier plan (outline who will do what, where, when, and how) at all FPCONs, then exercise actual execution to validate resource requirements and time needed to deploy the barriers.

f. Commanders need to be aware that barrier plans must be evaluated at least annually or against changing threat and/or terrorist tactics. By careful application of the barrier planning principles, the commander will establish an effective facility barrier plan that will greatly enhance protection from terrorist vehicle bomb attacks.

Appendix G, "Sample Barrier Plan," provides a sample barrier plan extract. It shows the type of information and layout desired to facilitate effective barrier planning.

5. Range-to-Effect Charts

a. The structural protection assessment determines the effectiveness of facility structures and layout to protect individuals from potential bomb blast effects. The information presented can be used by base personnel for self-assessment, permitting prediction of weapons effects on people and structures, and suggesting strategies to mitigate these effects. Consideration is given to construction types, proximity to roads, personnel concentrations, and their importance to base security and disaster recovery. A range of weapons yields is considered. Typically a 220 pound high explosive (HE) car bomb is selected for illustrative purposes in an assessment in CONUS, and is representative of the threat from an inspected-car bomb (i.e., 220 pounds of HE can be effectively hidden on a car despite inspection by trained personnel).

b. Figure VI-7 is the range-to-effect chart for a generic, conventionally constructed building with a reinforced concrete frame. This figure shows a family of curves with increasing damage and injury based on the size of the weapon and the distance from the weapon. The figure also reflects the two top priorities for structural protection: prevention of catastrophic structural collapse and reduction of glass injuries. The column damage curve is provided to help prevent catastrophic collapse such as occurred at the Murrah Building in Oklahoma City. The remaining curves represent varying Levels of Protection from injuries caused mainly by glass, although injuries from building wall fragmentation are also included for facilities with limited glass.

c. The range-to-effect chart provides an installation the capability to self assess. Based on this information, the commander can take appropriate action to implement procedures or changes to the base structures to reduce the weapon's effectiveness. For example, increasing the standoff from the weapon to the target building by closing roads during higher FPCONs would reduce the weapon's effectiveness.

d. Another use for the range-to-effect chart is an aid to the security operations center (SOC). The SOC could contain a scale map of the installation. During a bomb threat, the bomb's location and estimated size could be plotted on the base map and the best evacuation plan determined. The icons along the top of the chart may be helpful in estimating the size of the weapon. For example, Figure VI-8 shows typical building vulnerability radii plotted for a 220 pound terrorist vehicle bomb near a HQ building. The circles correspond to selected data presented in Figure VI-7. Once the bomb's location is reported to the SOC, an estimate of the bomb's size can be made, the weapons effects can be plotted, and a rational plan of action can be implemented.

e. The range-to-effect chart can also be used to develop iso-damage contours. An iso-damage contour shows the standoff distance around a facility required to prevent the specified level of damage or injury for a given bomb size. As an example, Figure VI-9 shows a barrier plan developed using iso-damage contours around the same HQ building and surrounding barracks. The contours were developed for a 220 pound car bomb threat using the information contained in Figure VI-7. The major options available for mitigating the effects of a bomb are

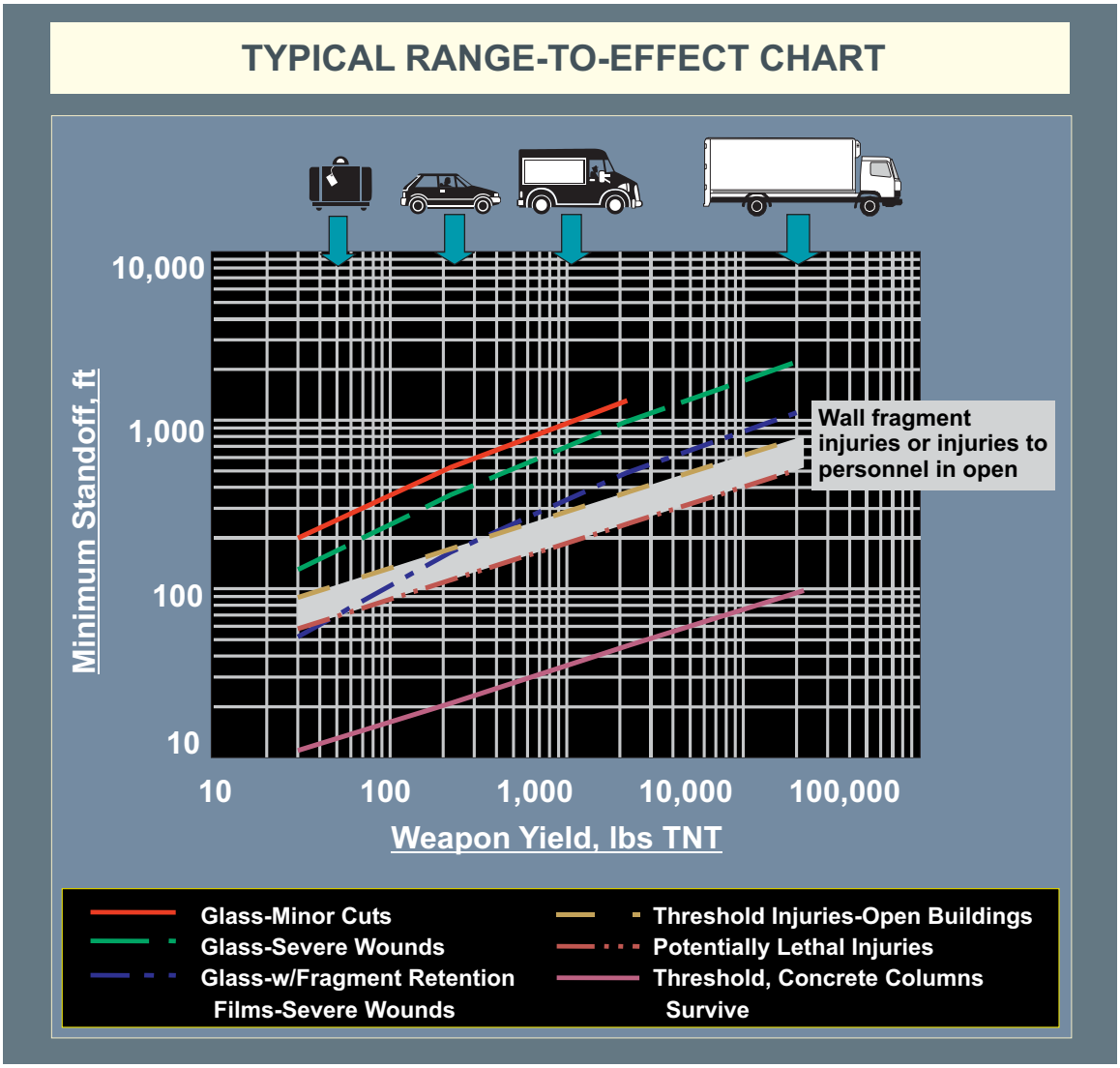


Figure VI-7. Typical Range-to-Effect Chart

keeping the blast source from the structure by maintaining standoff distance, or by upgrading the structure. This information assists the commander in developing a mitigation strategy with actions such as posting guards during increased threat periods; blocking access to nearby parking lots; closing roads; or increasing the building's blast resistance by upgrading the windows and doors. A good source of information for planning effective security measures is Army TM 5-853/Air Force Manual (AFMAN) 32-1071, *Security Engineering.*

6. Window Upgrades

a. Glass is usually the most vulnerable (i.e., weakest) part of a facility, with glass related injuries accounting for about 80% of the casualties from terrorist bombing events. Commonly used annealed glass behaves poorly when loaded dynamically. The failure mode for annealed glass creates large sharp edged shards, resembling knives and daggers. For the window assemblies

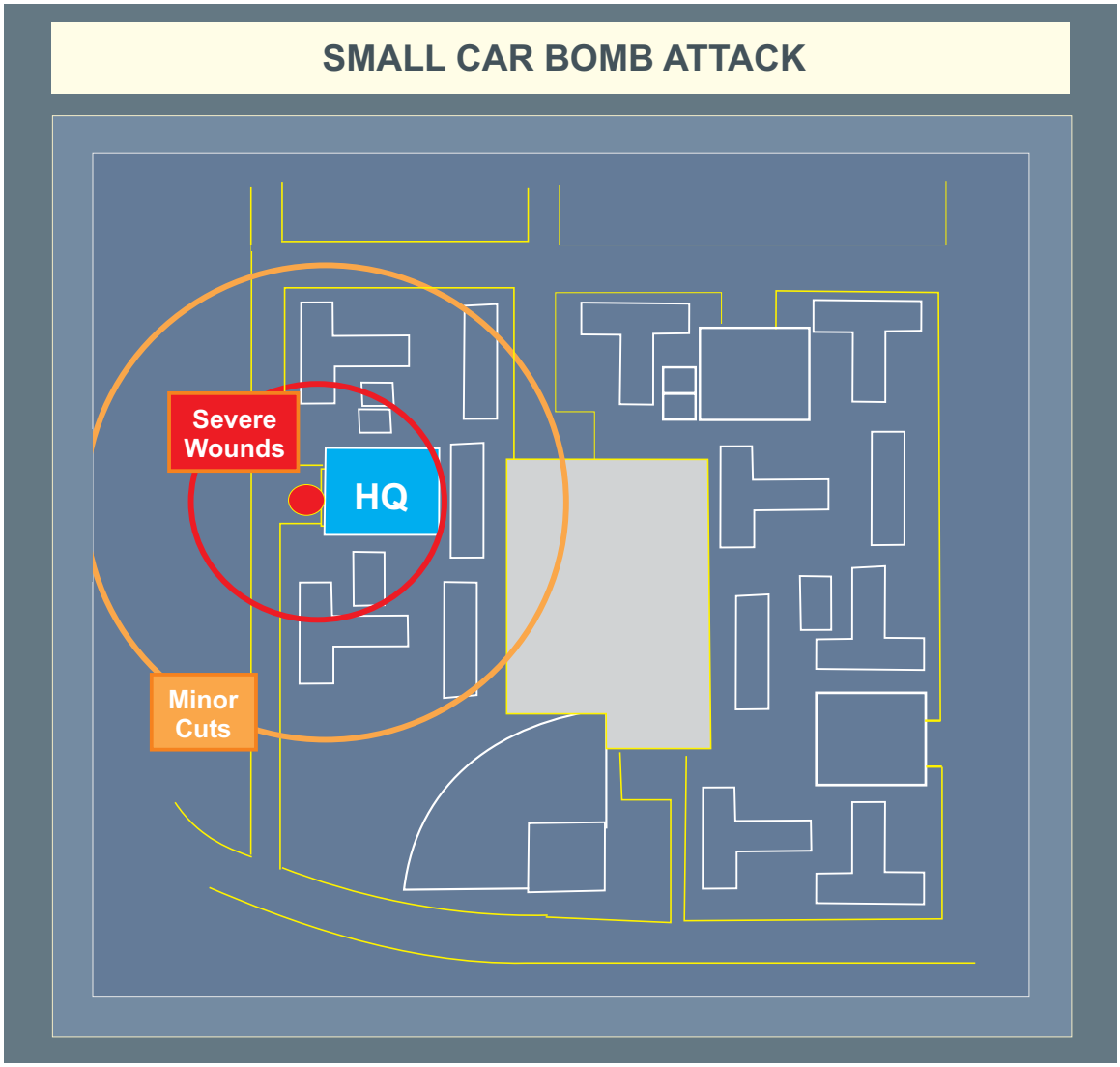


Figure VI-8. Small Car Bomb Attack

to behave properly, the glazing, frames, and anchorage must *all* be capable of resisting the blast pressures and transfer the loads to the adjacent structure.

b. Several possible actions could be taken to reduce glass hazards to people. For instance, if natural light is desired, glass block is effective at transmitting natural light while providing protection equivalent to an unreinforced concrete masonry unit wall. Alternatively, the use of security windows comprised of laminated, polycarbonate, or thermally tempered glass (TTG) with upgraded and well-anchored frames will provide a higher level of blast protection. Laminated and polycarbonate glass typically remain in one piece when they fail under higher blast pressures, demonstrating 5-10 times the blast capacity of annealed glass of similar thickness. They often pull out of their frames (or take the frames with them) and can cause injury similar to a large flying object. TTG breaks into rock-salt sized pieces that will inflict less injury on people.

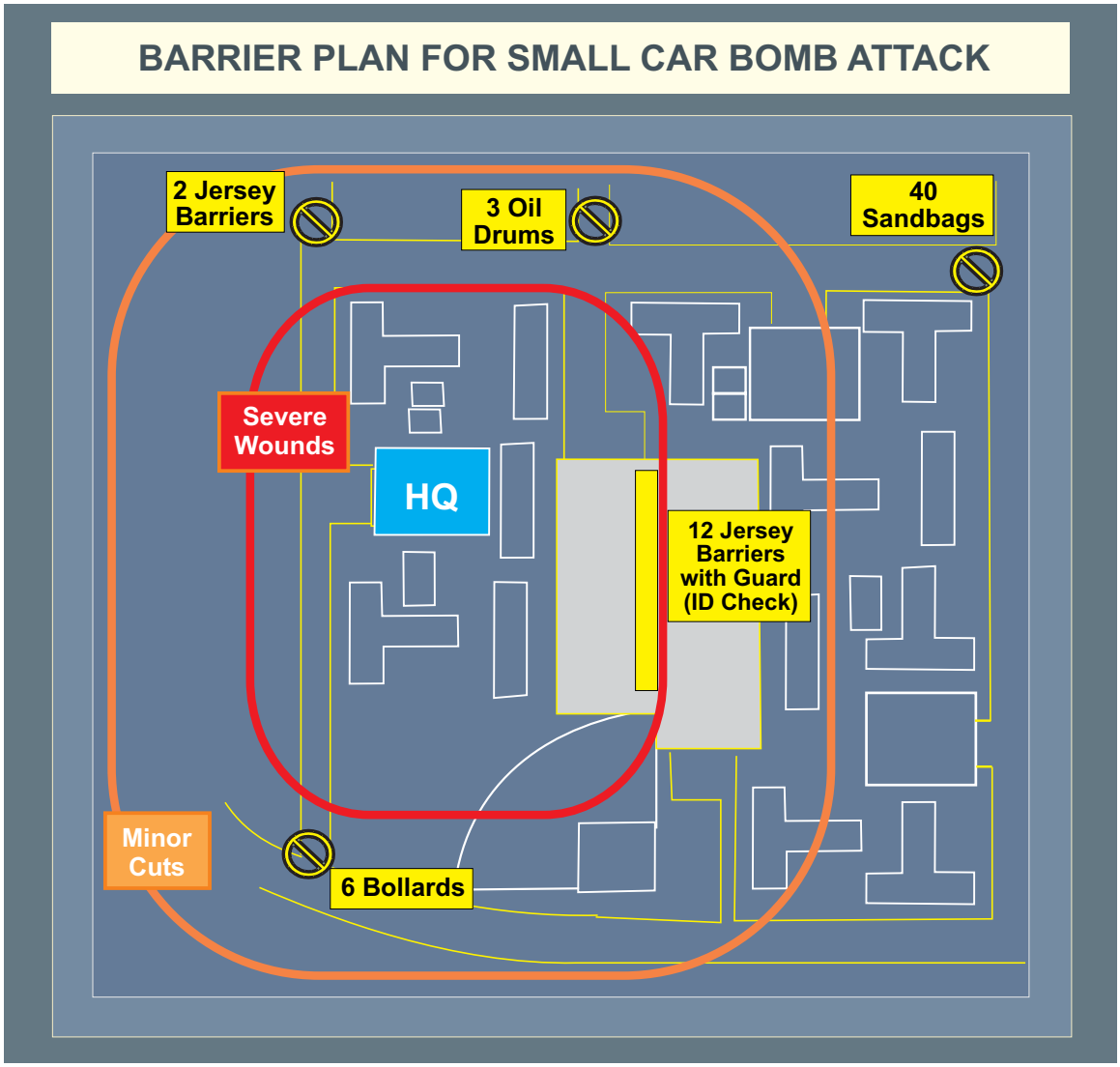


Figure VI-9. Barrier Plan for Small Car Bomb Attack

c. Fragment retention films (FRFs), i.e., Mylar can be used with existing frames to provide an economical (starting at approximately $4/ft^2 including installation for 4-mil FRF), but lower level of protection. FRF is designed to keep glass shards together, reducing the shredding effect of flying glass debris; however, these panels (plus lightly-anchored frames) can still be expected to be blown into rooms, potentially creating blunt trauma hazards. Proper application is critical to the performance of the film. The recommended method of application is to install the film to the outside edge of the glazing material and extend the film a minimum of 1/4-inch inside the frame bite. If this method is not possible, then the film should be installed to within 1/16-inch of the visible glazing edge (known as the "daylight" method). The limitation of the "daylight" installation method is that the glass will likely not be retained in the frame under blast loads; however, it will still reduce the level of fragments from the shattered glass.

d. A 4-mil thickness of FRF is recommended for the "daylight" installation method. A thicker film, up to 15 mils (approximately $10-11/ft^2), will increase the level of protection from

shattered glass provided that the film can be extended into and properly attached to the frame. In addition, the frame, the surrounding wall construction, and the connection of the frame to the wall must be analyzed to determine if they have sufficient strength to allow the increased thickness fragment protection film to perform to its design capacity.

e. Figure VI-10 demonstrates the significant benefits available from various glazing upgrades, using a scenario of a 220 pound vehicle bomb near a family housing area as an example. The contours represent the required standoff to prevent serious injuries. As can be seen, simply adding 4-mil FRF to a single-pane annealed glass reduces the required standoff 55%, dramatically reducing the area potentially affected as well as likely reducing the severity of injury. Upgrading to a security glazing system (such as thermally tempered or laminated glass) can reduce the standoff even more (see Figure VI-11).

7. New Construction and Renovation

a. The costs of including good AT principles into new construction and renovations are the least at the earliest design phases.

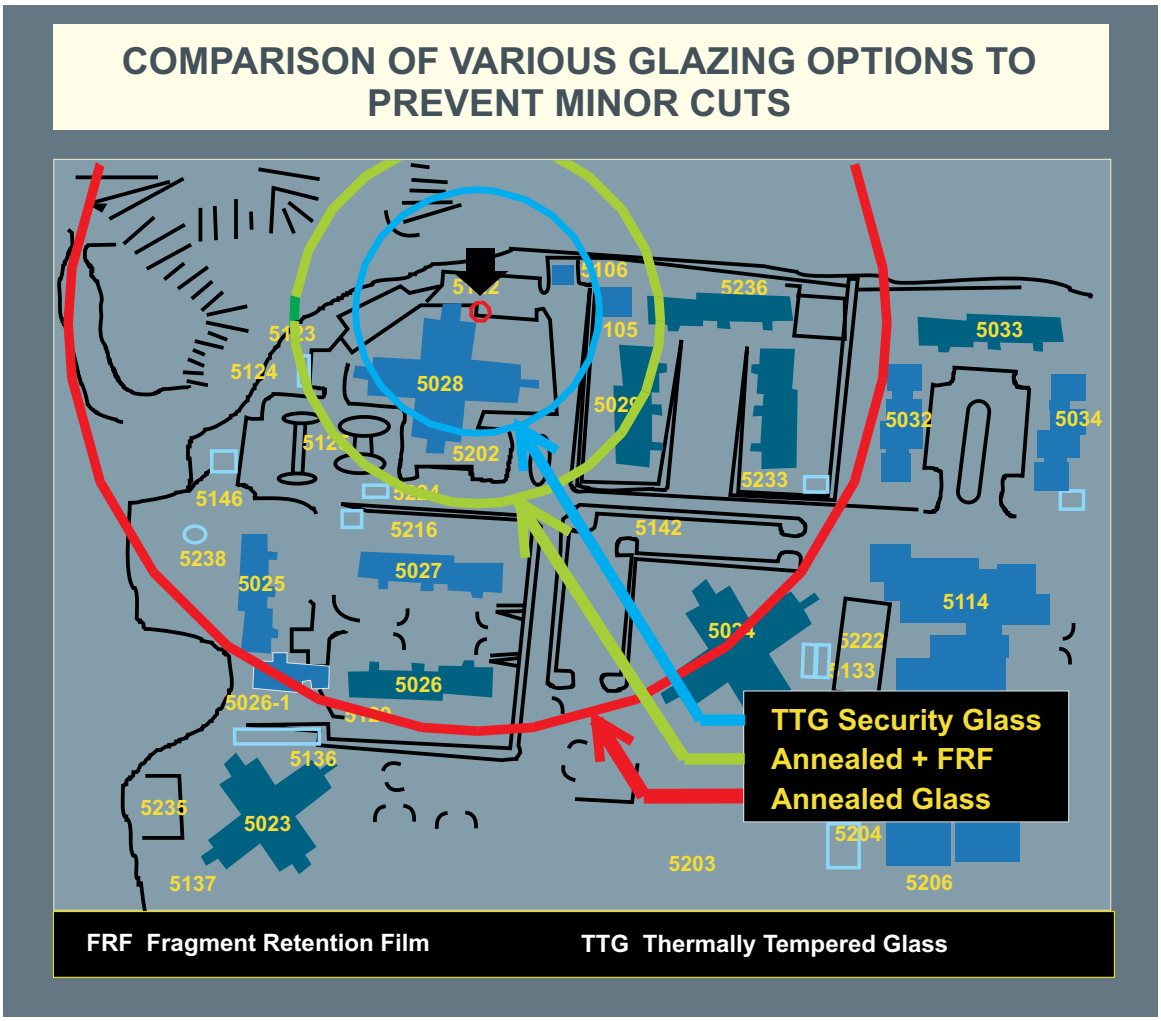


Figure VI-10. Comparison of Various Glazing Options to Prevent Minor Cuts

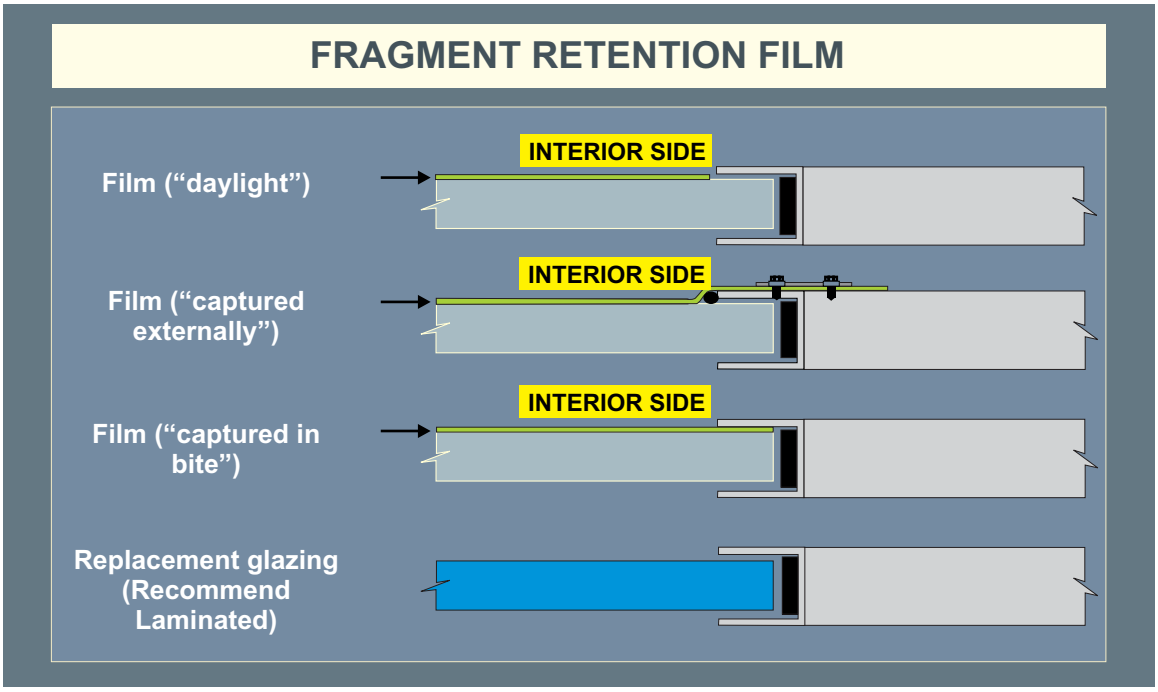


Figure VI-11. Fragment Retention Film

b. Listed below are some suggested design considerations. The DOD UFC 4-010-01, *DOD Minimum Antiterrorism Standards for Buildings*, and UFC 4-010-02, *DOD Minimum Standoff Distances for Buildings*, contain the current DOD standards for all new building construction.

(1) Maintain standoff.

(2) Locate construction staging areas away from buildings.

(3) Locate facilities away from installation perimeters.

(4) Eliminate vehicular lines of approach that lead directly into building entrances.

(5) Minimize vehicle and personnel access points.

(6) Do not provide parking beneath facilities.

(7) Locate parking as far from buildings as practical: consider use of exclusion zones, passive vehicle barriers, and speed control obstacles.

(8) Use blast resistant design (Note: Higher standards of earthquake or hurricane resistant design provide improved ductility and stronger frames, which improve blast resistance).

(9) Use interior courtyards when outside views and natural light are desired.

(10) Place storage areas, receiving areas, and mail rooms along exterior walls and more populated areas in the central portion of the building.

(11) Incorporate "safe haven" areas in the central core areas of the facility (i.e., interior stairwells).

(12) Minimize or eliminate window areas where practical; consider using more blast resistant window systems, especially glass block; consider placing windows six feet above the floor.

(13) Use steel doors and frames in foyers and entrances.

(14) Secure access to power and/or heat plants, gas mains, water supplies, mechanical rooms, and electrical service.

(15) Coordinate designs with organizations responsible for installation security and incident response.

8. Joint Rear Areas

During joint and multinational operations, US units and bases in the joint rear area (JRA) are still vulnerable to terrorist attacks. The same procedures identified in the preceding paragraphs apply. Commanders will be advised by the joint security coordinator (JSC) of potential terrorist threats, and subordinate commands will report any terrorist activity to the JSC. Units passing through the JRA are still required to maintain AT measures commensurate with the JSC's guidance. Specific TTP for operations in the JRA are contained in JP 3-10, *Joint Security Operations in Theater*.

9. Suicide Bombers/High Risk Vehicle Checkpoints

a. The purpose of this section is to highlight references and resources and capture best practices to enhance AT mitigation measures for conducting high risk vehicle checkpoints and deterring suicide bombers.

b. Vehicle borne bomb and suicide bomber attacks in OIF highlight this threat to our forces. Because of robust protective measures in place at DOD installations, our checkpoints and roadblocks are increasingly becoming prime targets for terrorists. Security personnel at access control points can also be targeted as a means to gain access to installations/compounds.

c. The land component command for OIF and the Service components established excellent TTP for dealing with high risk vehicle checkpoints and the suicide bomber. TTP, and lessons learned on Service and combatant command web sites and DIA JITF-CT assessments of terrorist tactics are excellent sources for commanders and AT officers to review. The following paragraphs provide information gleaned from component threat reporting, TTP, and lessons learned.

d. Threat Tactics

(1) Common Factors

(a) Terrorists use deception, such as feigning distress, to get close to target areas.

(b) Terrorists use multiple attack vehicles, first to breach the perimeter defense and then penetrate the target area.

(c) Terrorists conduct preoperational surveillance to identify weak points.

(d) Terrorists modify their tactics to overcome security measures.

IRAQI TAXI CAB

An Iraqi posing as a taxi cab driver feigned a breakdown and detonated his vehicle when four soldiers approached killing them all. Three rangers were killed in western Iraq when an SUV [sport utility vehicle] drove up to their check point (along with other cars) and then exploded. In another instance, an Iraqi at a checkpoint set off explosives hidden under his clothes wounding a number of Marines. In all cases, deception was used to get close to US forces and increase the effect of the attack. This tactic is continuing to be used by enemy paramilitary during the stability phase.

Various Sources

SAUDI ARABIA

The terrorist attacks on 12 May 2004 against three residential housing compounds in Riyadh, Saudi Arabia occurred minutes apart using the same method. In each attack, an assault element was used to breach the compound gate, enabling another element to drive a vehicle-borne improvised explosive device to a pre-selected target on the installation where it was detonated.

Various Sources

(2) Suicide bomber threat. All individual suicide devices are based upon the simple concept of using a human being to deliver a bomb to a target. Generally, the bomb will have the following characteristics:

(a) A simple switch for initiation consisting of a push-button or toggle switch completing an electric circuit. Relatively small initiation devices reduce the chances of discovery.

(b) Fragmentation such as nails, ball bearings, or other small metal pieces. Dispersed fragmentation is the primary kill mechanism in individual suicide bombing attacks.

(c) Devices are generally concealed within an article of clothing worn close to the body — such as a vest, belt, or jacket. However, there have been instances where the explosive device is disguised to look like a common, innocuous object.

(d) Plasticized explosive as a main charge — usually a homemade mixture, although groups with access to greater resources utilize military grade explosives.

(e) Many devices have a backup trigger system, such as an electronic timer, pager, or booby-trap type switch. If the attacker is killed, apprehended, or attempts to abort the attack, a secondary trigger system provides an alternative initiation method.

(3) Possible indicators of a suicide bomber are as follows:

(a) An individual who deliberately ignores orders to stop or attempts to circumvent a security checkpoint.

(b) An individual wearing too much clothing for the prevailing weather conditions.

(c) A person with suspicious bulges in his or her clothing, carrying packages/bags, wearing satchels/backpacks or walking with unsteady gate.

(d) Individuals may exhibit a wide range of characteristics, such as clean shaven with closely cropped hair, exhibit unusual emotional demeanor such as blank stare, grin, unresponsive, and may perspire or appear gaunt and/or ill.

(e) An individual handling wires, switches, an actuator, or a dead mans switch; or using an overly intense grip on any object.

(4) VBIED threat. A VBIED is a vehicle modified to conceal and deliver large quantities of explosives to a target. The motive behind such incidents is to cause many casualties and gross property damage. Possible indicators of a VBIED threat are as follows:

(a) Noticeable sagging of the vehicle on its springs caused by the heavy weight of explosives found in it. Ordinarily the explosives will be placed toward the rear of the vehicle, causing it to ride lower in the rear. However, sagging springs are not normally characteristic of trucks being used for VBIEDs because these vehicles are designed to carry the weight.

(b) Darkened or covered windows to conceal either the vehicles contents or the actions of the driver.

(c) Unusual items inside the vehicle: gas cylinders, wires, leaflets, large bags or boxes, and batteries besides the normal car battery.

(d) Indications of a triggering device — e.g., a switch, radio transmitter, timer, wires, or ropes passing from the front seat to the rear of the vehicle — visible near the driver, under the seat, or within arms reach.

(e) The presence of the vehicle in an area where it should not be, perhaps illegally parked.

(f) Holes made in the vehicle body to hide explosives and then crudely covered.

(g) Evidence that an interior door panel has been removed to hide explosives.

(h) The presence of powder or prills (small rounded granular material) left when explosive material was loaded into the vehicle.

(i) Recent painting of the vehicle to cover body alterations.

(j) Additional fuel tanks, used to secrete explosives or to provide additional gasoline to fuel the explosive event.

(k) Unusual smells, e.g., a burning time fuse, gasoline, fertilizer

(l) An additional antenna on the car for radio-controlled devices.

(m) Any disturbance to the undercoating or dirt on the bottom of a vehicle.

(n) Indications that drivers may be associated with VBIED are as follows:

1. Driving erratically; driving too slow or too fast.

2. Ignoring orders to stop, attempting to circumvent a security checkpoint, or attempting to maneuver too close to coalition assets.

3. Wearing inappropriate dress or grooming for the vehicle type.

4. Signs of nervousness, sweating, shaking, or unusual speech patterns.

5. The presence of a lone driver in the vehicle. This is standard for VBIED operations; however, there could be any number of people in the vehicle if the VBIED is being driven by an unsuspecting person.

6. Inability to operate the truck or equipment properly.

7. Atypical appearance. Terrorists may be uncharacteristically clean-shaven and have very short haircuts. Cutting the hair is a part of the purifying ritual that many follow prior to an attack.

8. Age: mid-twenties. The average suicide terrorist is about 24 or 25, but age is not a definitive discriminator.

(o) Other suspicious conditions:

1. Occupants careful when closing the doors.

2. Vehicle left locked and unoccupied.

3. Not obviously engaged in loading or unloading.

4. Displaying hazard warning lights.

5. Parked near or adjacent to an important target.

6. Illegally parked.

(p) Common areas for concealing VBIED explosives:

1. Above roof liner.

2. Behind door panels.

3. In spare wheel well.

4. In hollowed-out seats.

5. Under false flooring.

6. Inside fuel tank (smaller alternate fuel tank elsewhere).

7. In legitimate cargo area — such as trunk, trailer, or storage bin.

8. In legitimate packaged cargo.

(q) General safe blast/fragmentation distances for VBIED have been determined to be as follows:

1. Compact sedans can carry up to approximately 500 pounds (227 kilos) of explosive. This gives a lethal blast range of approximately 30 meters, and a fragmentation hazard of 381 meters.

2. Full-size sedans can carry up to approximately 1,000 pounds (455 kilos) of explosive. This gives a lethal blast range of approximately 38 meters, and a fragmentation hazard of 534 meters.

3. Passenger or cargo vans can carry a maximum of 4,000 pounds (1,818 kilos) of explosive. This gives a lethal blast range of approximately 61 meters, and a fragmentation hazard of 838 meters.

4. Small box vans (14 ft) can carry a maximum of 10,000 pounds (4,545 kilos) of explosive. This gives a lethal blast range of approximately 91 meters, and a fragmentation hazard of 1,143 meters.

5. Box van or water/fuel trucks can carry a maximum of 30,000 pounds (13,636 kilos) of explosive. This gives a lethal blast range of approximately 137 meters, and a fragmentation hazard of 1,982 meters.

6. Semitrailer can carry a maximum of 60,000 pounds (27,273 kilos) of explosive. This gives a lethal blast range of approximately 183 meters, and a fragmentation hazard of 2,134 meters.

e. The following TTP may prove effective deterring, disarming or mitigating pedestrian suicide bomber attacks

(1) Visual observation remains the primary method of detecting suicide bombers. Screening methods can also be employed such as having suspects open their coats or lift shirts at a safe distance before approaching a checkpoint. Thermal images have proven effective for standoff detection of concealed weapons on personnel, provided that external clothing is not too heavy. These items serve as a heat sink (i.e., block radioactive emissions) and therefore are rendered as distinct spots on thermal images. This technique may prove effective for detecting concealed explosives but has not been tested in this role.

(2) If a bomber is identified, orders should be issued to evacuate the area immediately (minimum of 50 meters away) and to take cover (behind substantial barrier). Safe distances depend upon the mass of explosive carried by the bomber and the amount and type of fragments used. Distances will necessarily be constrained in urban conditions but safety zones must be considered when selecting checkpoints or establishing gate operations. It should always be assumed that fragments are part of the charge as safe standoff distances are greater for fragments than for blast.

(3) If a bomber is identified, security personnel should train weapons on the bomber and maintain eye contact from behind cover. Ensure fields of fire have been identified and rehearsed to avoid fratricide and endangering innocent bystanders.

(4) Separate the subject from the IED: warn target that failure to comply will result in the employment of deadly force. Order the target to remove outer garments, place them on the ground, and then stand with hands raised. Have subject move a safe distance away from clothing and then handcuff.

(5) Assume a fail safe cell phone or radio-controlled initiator could be used in the event that the bomber is incapacitated or hesitates. This tactic would normally involve a second suspect with a LOS view of the bomber. Consider surveillance detection efforts to monitor the environment and deter enemy observers near the checkpoint or gate.

(6) If deadly force is employed, bullet impact may initiate the explosive charge(s). Therefore firing on the suspect should be undertaken from cover and not be aimed at mid-body.

(7) If the suspect is neutralized and there is no explosion, do not administer first aid. The explosive charge should be rendered safe by authorized EOD personnel only.

f. The following are TTP to consider to mitigate the VBIED threat at high risk vehicle checkpoints

(1) Elements

(a) A headquarters element to ensure command and control.

(b) A security element to provide early warning and observe flow of vehicles approaching the checkpoint.

(c) Traffic sentry to operate stop point forward of and controls traffic leading to checkpoint. Signs in the local language should be used to communicate instructions for negotiating barriers leading to search location.

(d) Search team to halt vehicles, conduct searches, and direct cleared vehicles onward. One member should search the vehicle while the other team members provide over watch.

(e) An assault element in fortified positions to overwatch checkpoint. This element should be prepared to engage (consistent with ROE) any vehicle that attempts to force its way through or poses a danger to the checkpoint.

(2) Checkpoints should present a robust security posture in order to discourage threats. Consider employing armored vehicles and crew served weapons in overwatch positions to support dismounted troops. Consider an antiarmor capability for security elements.

(a) A serpentine vehicle maze (barriers/freeway dividers) can be used to slow vehicles approaching the search area. A vehicle maze will enable security personnel more time to react to a vehicle attempting to run or attack the check point, as well as channel threat vehicles in escape lanes to a predetermined location for engagement.

(b) Hasty checkpoints should take advantage of terrain features/surrounding obstacles (bridges, highway/road intersections, reverse slope of a hill, just beyond a sharp curve) to slow vehicles as they approach the checkpoint. Deliberate checkpoints may require engineers

or other support to emplace obstacles and barriers to channel traffic. Deliberate checkpoints should include holding/search areas with appropriate blast protection for personnel conducting searches.

(3) Suggested procedures

(a) Instruct passengers to get out of the vehicle at a pre-designated and well-marked search area.

(b) All passengers should be instructed to come out with arms above their heads. Once out of the vehicle, instruct male passengers to lift their shirts in order to enable security personnel to observe waist. If there is doubt, have them strip.

(c) Instruct one passenger to open all doors, hood, and trunk.

(d) Consider that women and children have also carried out attacks and ensure they are disarmed as well. When available, use female US military/HN security personnel to search females, preferably in a separate, closed area.

(e) If any member or personnel at the checkpoint has any doubt about the vehicle, back everyone off and call for assistance.

(4) Suggested equipment — the following are mission enhancing tools at a high risk checkpoint.

(a) Loud speaker team with linguist. When linguists are not available, consider using recorded audio warnings. Time permitting, prepare and emplace signs in the local language instructing drivers what to expect and do at the checkpoint.

(b) Explosive detector dog teams.

(c) Use of metal detector wands for physical searches, if possible, in addition to a crush and feel search.

(d) Stingers/caltrops (device that can be dragged across the road to puncture tires).

(e) Vehicle control and blast mitigation barriers.

(f) Separate search areas for small and large vehicles. Consider using trenches large enough for vehicles to enter so they may be searched. Vehicles can pull into the ditch and open all doors prior to search.

10. Airfield-Specific Threats

a. **Airfield security and local area assessments** should be conducted to identify the areas of vulnerability to direct fire, indirect fire and shoulder launched surface to air missile threats (in terms of possible launch sites) to include the airfield arrival and departure corridors. A thorough assessment should include the capabilities of security personnel, intelligence, CI, and operational personnel as well as local/HN authorities.

(1) Criteria to identify possible direct fire, indirect fire and shoulder launched surface to air missile launch sites include but are not limited to

(a) Cover and concealment — the ability of an object to conceal and prevent detection by friendly forces, and to provide protection for the adversary from return fire.

(b) LOS providing unobstructed view of the target.

(c) Exposure time — the amount of time the intended target is vulnerable from an operational attack.

(d) Distance to target and the range of the adversary's weapons systems as well as target recognition for the adversary to positively identify the intended target.

(e) Set up time required for an adversary's fire team to assemble into an attack position.

(f) The amount of time it takes to detect an adversary' fire team once their weapons are exposed.

(2) Because potential launch sites may be located some distance outside the existing base or installation fence-line, base commanders and area commanders share the responsibility to protect airfields from attack. Both must coordinate defensive efforts and allocate resources to detect, deter, and destroy this threat to airfield operations and personnel.

(3) The preferred method would be to deny an attacker access to potential launch sites, however that may not always be possible. Develop and exercise contingency plans for responding to an incident of direct fire, indirect fire or shoulder launched surface to air attack. Rapid reaction plans will facilitate the immediate capture of a terrorist team, even post attack, to deter/prevent future attacks and ease concern for air travel safety by the public at large.

b. **Direct and Indirect Fire Threats**

(1) Vulnerability assessments should be conducted to identify the areas from which direct and indirect fire threats can attack lucrative ground targets such as mass gathering areas, parked aircraft, or vehicle motor pools.

(2) Consider dispersal of parked aircraft to reduce damage from direct or indirect fire attacks, such as rocket propelled grenades.

c. **Shoulder Launched Surface to Air Missile System Threats**

(1) The Defense Intelligence Agency-Missile and Space Intelligence Center has flight path threat analysis simulation (FPTAS) software that allows the local commander to quantify the areas of greatest shoulder launched surface to air missile threat. FPTAS uses aircraft performance, flight path data, missile characteristics, and digital terrain elevation data to generate maps depicting area from which shoulder launched surface to air missile could engage US and allied aircraft. Commanders have used these maps to identify flight paths with minimum exposure to the shoulder launched surface to air missile threat and have adjusted take off/landing patterns to limit their exposure and utilize areas readily secured by ground troops. This software can be downloaded at the following web site: http://msic.dia.smil.mil/ms_home_page/fptas/.

(2) Air Mobility Command (AMC). AMC intelligence maintains a database with current intelligence and operations information on select countries and airfields, to include a shoulder launched surface to air missile TA. This assessment is used to determine the requirement for aircraft defensive systems to counter the shoulder launched surface to air missile threat; and on a more basic level, to determine whether nondefensive system equipped AMC military and commercial aircraft will be permitted to operate into those countries or airfields. This information can assist the air component commander in making their own policy decisions for aircraft operations at those same locations.

(3) There are two areas where commanders and AT officers should employ mitigation measures to counter the shoulder launched surface to air missile threat: airfields/installation defense and reducing aircraft in-flight susceptibility.

(a) The following are points to consider in developing AT plans in regards to airfield/installation defense and the shoulder launched surface to air missile threat.

1. Once an analysis of possible launch sites is accomplished, prime shoulder launched surface to air missile launch sites and vulnerable areas can be isolated by expanding the airfield area of control and reducing areas of vulnerability. The following mitigation measures may require coordination with local/HN authorities:

a. Increased physical presence at prime launch sites. Visual observation of security teams is a strong deterrent.

b. Focused and random patrols of potential launch sites. Incorporate random patrols into the installation random AT measures program.

c. Employment of technical equipment to detect and respond to the various threats.

2. Ensuring personnel are educated on the shoulder launched surface to air missile threat (to include component recognition), areas of vulnerability, and reaction plans. Develop and provide shoulder launched surface to air missile awareness training for security force personnel and local/HN authorities. Develop a shoulder launched surface to air missile awareness program for neighborhood watch groups and local business/installation facilities in close proximity to airfields or along flight paths. The Defense Intelligence Agency Missile and Space Intelligence Center has a web site in their Operation ENDURING FREEDOM section with a shoulder launched surface to air missile link that is a good source of information on shoulder launched surface to air missile systems (http://msic.dia.smil.mil/ms_home_pages/SAM/SD_Home_Page.html).

(b) To reduce aircraft in flight susceptibility due to the shoulder launched surface to air missile threat, consider the following when developing AT plans:.

1. Establishing airfield specific procedures for the use of aircrew tactical countermeasures and/or tactics. Development and dissemination may require coordination with local/HN authorities. Ensure aircrew awareness of launch identification and the possible effects of shoulder launched surface to air missile on their aircraft. Ensure aircrews and flight operations are tied into the AMC intelligence combined risk assessment database to obtain current information on airfield security assessments.

2. Varying arrival and departure times of aircraft. Stagger the arrival times of normal scheduled missions to make arrival, departure, and ground times harder to predict for the adversary.

3. Randomly change approach and departure routes as a deterrent (in accordance with current Federal Aviation Administration guidelines).

4. Limit or discontinue use of landing lights within identified threat zones to reduce heat producing/targeting options.

5. In high threat areas or when intelligence has indicated a high alert status, coordinate, develop, and practice plans for engine-running offloads to minimize ground time.

11. Information Operations

a. IO are part of the FP concept and complement AT efforts, especially in locations outside the continental United States.

b. IO are actions taken to affect adversary information and information systems while defending ones own information and information systems. They apply across all phases of an operation, the range of military operations, and at every level of war. Properly managed IO offer dynamic AT benefits by creating an information environment around the installation that recognizes and negates enemy propaganda or activities, facilitates trust and interaction with the community, and ultimately increases and assures effectiveness of C2 efforts.

JP 3-13, Information Operations*, provides doctrine and a detailed discussion of IO.*

12. Community Engagement

a. Historically, an adequate AT posture meant an established perimeter, guarded access points, random antiterrorism measures, and other defensive actions consistent with the AT program. Complementing these measures and related to information operations, community engagement is a tool that can be employed at the tactical level outside the perimeter by both garrison and forward deployed commanders (see Figure VI-12). Community engagement is the result of lessons learned by troops deployed to Iraq, Afghanistan, and the Balkans. Essentially, when deployed, US forces become part of the local community and local interaction at various levels can either improve or decrease the force protection posture of the forces. Community engagement is a means to acknowledge the local nationals' role and standing in their own neighborhood and demonstrate the discipline, confidence, and professionalism of US forces. The concept of community engagement grew from the traditional tactical practice of establishing listening/observation posts (LP/OPs) when in the defense. Once the community and US roles are established and the informal relationship and mutual respect emerges, the community will serve as informal LP/OPs for the US location. Community engagement is defined as: the process of increasing

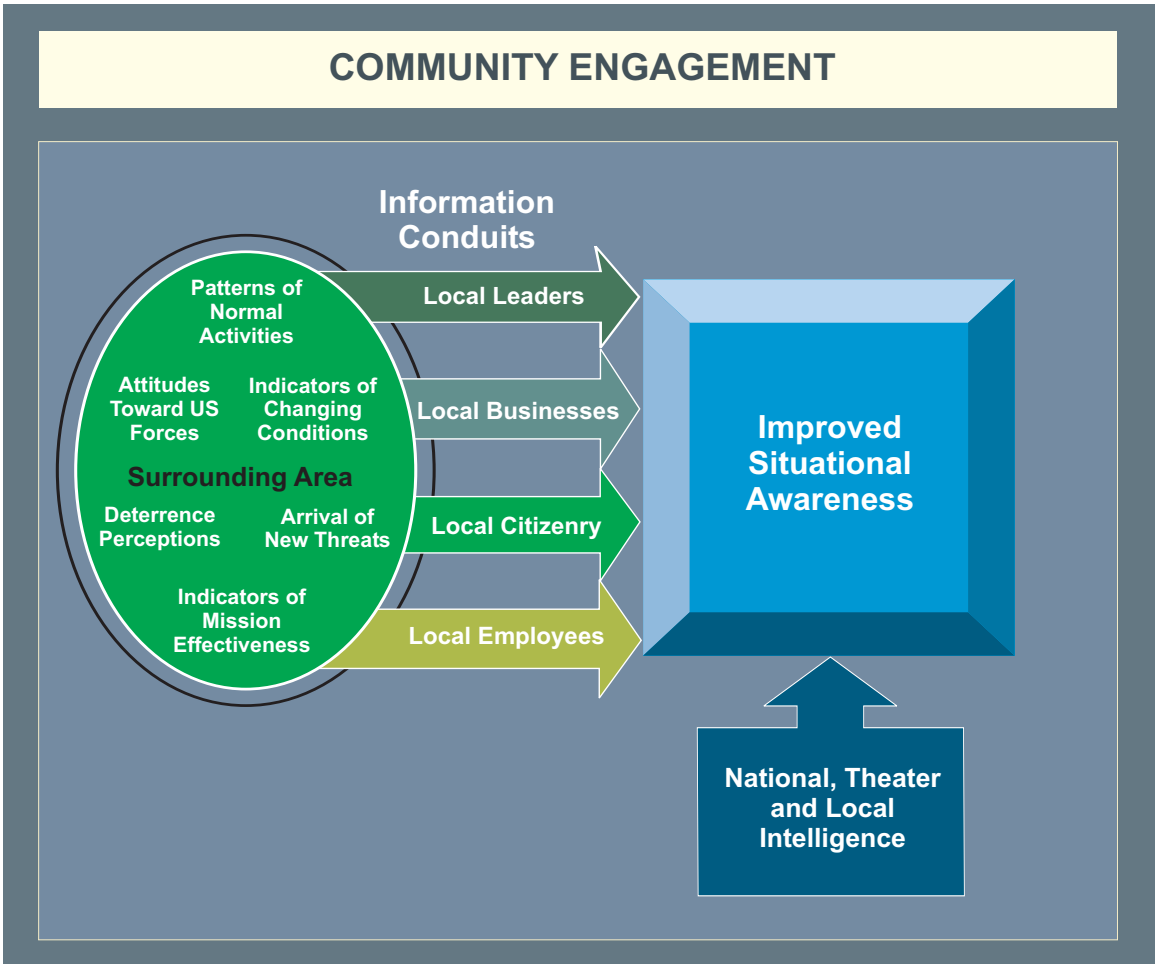


Figure VI-12. Community Engagement

the commander's capability to define the local threat picture using improved situation awareness of the surrounding area, and developing a defense in depth. Community engagement is never the mission. It is tactical, an enabler that facilitates both force protection and accomplishment of the primary mission under appropriate conditions.

b. The principles of a community engagement strategy are planning, training, intelligence, and local community interaction. They are interdependent and mutually supporting.

(1) Planning focuses on how best to apply the principles and methods of engagement with the resources available, threat environment, host nation agreements, risk assessment, and mission objectives. Planners should draw on the range of players in the local community to include representatives such as NGOs, IGOs, and any multinational partners. All of these organizations can be leveraged to help the commander develop a more robust threat assessment built upon a fusion of national, theater, and local formal and informal intelligence. By planning, the commander is preparing not only to shape but also to respond better the the environment through interaction with the host nation population in order to counter threats more effectively.

(2) Training is the cornerstone of community engagement. Training starts with garrison or pre-deployment activities oriented to the region, people, culture, history, and conflict. Once deployed, training continues to refine knowledge of the operational area based on threat and local changes.

(3) Intelligence is integral to performing a detailed threat analysis. The threat analysis will assist commanders in determining which methods of community engagement are most appropriate. To perform a sufficient threat assessment, we must recognize that intelligence provided from national and theater levels may not provide sufficient detailed localized information that supports day-to-day decision making. The commander must fuse national intelligence information with information garnered through local community engagement. Key to the intelligence principal is the premise that every military member is part of the intelligence effort. Effectively employing the force to develop an accurate intelligence picture requires supporting analysis and fusion, but provides the commander with a mechanism that is highly sensitive to shifts in the environment. Every time US personnel enter the community, they must be aware of the information requirements, understand the message theme or perception the commander is intent on transmitting to the local populace.

(4) Local community interaction is the point where the US force enters the community and puts planning, training and intelligence preparation to the test. It is also the principal under which unit individuals build rapport with formal and informal community and entity leaders. It is through community interaction that threat entities are denied complete freedom of movement, crises are avoided or mitigated, and critical information is gathered allowing a commander to shape and respond better to the environment. As interaction with the community matures, a measure of force protection is gained.

c. Methods of community engagement. Increased access to and insight within the local community is self reinforcing, providing greater opportunities to engage and understand the

local environment. A by-product of improved situational awareness is an improved AT posture that allows commanders to effectively shape the environment. Methods of improving interaction and establishing rapport with the local populace may include but are not limited to:

(1) Limited unit language and cultural awareness training.

(2) Developing area study material.

(3) Establishing a focal point for fusion of national intelligence with local information.

(4) Developing a theme or goal for local interaction, which is consistently portrayed. All assigned troops are the most important means and venue of communication for this message.

(5) Improving methods of synergizing NGO/IGO and civil authority actions with US forces objectives.

(6) Development of a venue (radio channel, telephone line, note box, email address) for locals to report issues (such as inadvertent damage, follow-up to meetings, suspicious activity). The same line could be used as an anonymous tip line.

(7) Distribution of disposable cameras.

(8) Public community meetings to discuss current events, local needs, US local intentions, etc.

d. By pushing into the area surrounding US locations and developing positive informal relationships with local inhabitants, the terrorist freedom of movement is reduced and the probability of detecting threat movement is increased. Community engagement better enables US forces to recognize and counter terrorist information operations. The alternative is to keep US forces restricted to a confined perimeter, away from local populace and perpetually portrayed as a foreign occupant not a member of the community. By confining the US military presence to a given perimeter, garrison, or ship, the surrounding battlespace is surrendered to the enemy. Overall, community engagement increases mutual understanding, reduces uncertainty, deters aggression, increases rapport, and helps relieve sources of instability before they become military crises.

CHAPTER VII
INCIDENT RESPONSE AND CONSEQUENCE MANAGEMENT

"If historical experience teaches us anything about revolutionary guerrilla war, it is that military measures alone will not suffice."

BGen S.B. Griffith, USMC
Introduction to *Mao Tse-tung on Guerrilla Warfare*, 1961

1. General

a. **Incident response management** is a sequence of command, staff, and first responder actions to respond to a terrorist, natural disaster, or other manmade accident or incident or other unique event and restore AT capability. The primary objective of incident response management is to mitigate the effects and number of casualties resulting from a terrorist attack. Commanders develop response measures to save lives, preserve health and safety, secure and eliminate the hazard, protect property, prevent further damage to the installation, and maintain public confidence in the installation's ability to respond to a terrorist incident. Homeland Security Presidential Directive-5 mandated the use of National Incident Management System (NIMS) using the Incident Command System (ICS).

b. **Consequence management** is the preparedness and response to mitigate the consequences of an incident, including the use of CBRNE agents. It includes mass alerting or notification capabilities, disaster planning, public health, medical surveillance, and other preparatory efforts.

c. A commander's responsibility and authority to enforce security measures and to protect persons and property is utmost in importance during any level of conflict. As such, it is incumbent upon the commander to plan for, and be capable of reacting to, a terrorist attack. Attacks employing CBRNE weapons may produce massive casualties or widespread destruction, which can quickly overwhelm organic resources. This situation is covered in more detail later in paragraph 5 of this chapter.

d. The focus of incident management is on the organic assets of an installation, ship, or unit and the ability to cope with the situation using organic assets until outside assistance arrives. DODI 2000.16, *DOD Antiterrorism Standards*, requires all commanders to prepare installation-wide terrorist incident response measures and include them in the AT plan. The terrorist incident response measures should include procedures for determining the nature and scope of incidence response; procedures for coordinating security, fire, and medical first responders; and steps to reconstitute the installation's ability to perform AT measures. To be effective, incident response measures must be fully coordinated, exercised, and evaluated. DODI 2000.18, *Department of Defense Installation Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive Emergency Response Guidelines*, provides the specific requirements for response to CBRNE incidents.

e. There are an unlimited number of potential terrorist incidents requiring a response. Developing separate courses of action for each is an unrealistic task. To prepare for the most probable, or likely threats, AT plans should address (at an absolute minimum) each potential threat identified through the threat assessment process. AT plans should also maximize the use of existing plans and not reinvent SOPs. For instance, existing procedures for fire response, operation center management, disaster response, CBRN/hazardous materials (HAZMAT) response, security operations, and other related activities can be referenced in the document and do not need to be reproduced. The goal is to have a useable document that provides reference to needed information.

2. Incident Management Planning

a. The establishment of a mechanism to respond to a terrorist incident is an essential element of the DOD AT program. Normally, the installation, ship, or unit commander identifies an office or section, or designates personnel from various sections, who act as the principal planning agency for special threats and who comprise the emergency operations center (EOC) (see paragraph 3.d.) during an actual crisis. One effective method for determining what areas should comprise the planning and execution of the response is to use the WMD response functions.

b. There is no requirement to have a separate incident management plan. However, DODI 2000.16, *DOD Antiterrorism Standards*, requires that the AT plan address terrorist incident response measures.

3. Initial Response

a. **Onset of a Terrorist Incident.** The onset of a terrorist incident begins with the detection of an unlawful act of violence or threatened violence. Detection may result from routine surveillance performed by an installation or facility intrusion-detection system, guard or security force, or an unusual incidence of an infectious disease. In the case of bio-terrorism, an unusual incidence of an infectious disease may be an indication of terrorist activity. Once detection of a criminal act occurs, first responding security or LE personnel must perform an initial assessment.

b. **Initial Response Force**

(1) The initial response force consists of the forces identified in the installation's/ship's terrorist response plans with on-scene command relationships and chain of command clearly established in the same sources. At facilities controlled by the DOD agencies, the initial response force may be under the control of a senior civilian security official, or DOD LE official, or senior fire official. Once the initial response force has responded to the incident and determined the circumstances, the installation commander should activate required forces and begin notification procedures for military and civilian authorities.

(2) The initial response force should immediately identify and report the nature of the situation, isolate the incident, and contain the situation until relieved by the reaction force commander. Initial response force actions are critical. All installations/ships must have trained

personnel who are aware of the threat and are capable of reacting promptly to any new development 24 hours a day.

(3) For example, if the attack is a bombing, ambush, assassination, or firebombing, the terrorists may escape before additional forces arrive. In these cases, the initial response force should provide medical aid, seal off the crime scene, and secure other potential targets in case the initial attack was a diversionary tactic. If the event is a hostage/barricade situation, the initial response force should seal off and isolate the incident scene to ensure no one enters or leaves the area. The initial response force must also be prepared to locate witnesses and direct them to a safe location for debriefing. The initial response force must also be prepared to interface with local LE or emergency service personnel, HN police, or military forces responding to the incident in accordance with existing HNS MOAs and/or SOFAs.

c. **Installation/Base Commander.** The installation/base commander, depending upon established SOPs should activate the installation's EOC. Additionally, the commander should notify specialized response forces, and immediately report the incident to the appropriate superior military command EOC, military investigative agency, FBI, civilian authorities, and if a foreign incident, to HN authorities and the US embassy, as required.

d. **Emergency Operations Center**

(1) The EOC coordinates information and resources to support a terrorist incident response. EOCs should include the following core functions: coordination; communications; resource dispatch and tracking; and information collection, analysis and dissemination. EOCs may also support multi-agency coordination and joint information activities. Include in the EOC SOPs how communications are established immediately with the initial response force at the incident site and how specially trained operational response forces preparing to take over or augment the initial response force and other critical participants are incorporated into the EOC planning decisions.

(2) The EOC should distribute responsibilities into four basic functions:

(a) Operations. Responsible for first responders (fire, security, and medical); HAZMAT; bioenvironmental engineering; safety; and public affairs.

(b) Logistics. Responsible for service (communications, power, food) and support (shelters, supplies, etc.).

(c) Planning. Responsible for amending and developing plans to address the changing circumstances. Planning integrates a wide spectrum of interagency information and intelligence data into the overall effort.

(d) Administration. Responsible for tracking personnel casualties or fatalities, notifications, report, and contracting services as necessary.

(3) EOC emergency support function personnel should utilize available subject matter experts via a reachback capability. One source is the DTRA operations center (OC). This OC provides first responders and warfighters with information on CBRNE threats through on-line assistance, including hazard analysis and prediction modeling, and provides a wide-band infrastructure for user support. The DTRA OC is manned 24/7 and has the requisite links to act as the single point of contact for on-line assistance and dispatching of other DTRA resources, as required.

e. **Confirmation**

(1) Since jurisdiction depends on whether the incident is terrorist related, it is important for the response force to identify the type of incident as quickly as possible. If the FBI or HN assumes control, then the response force must be prepared to coordinate the operational handover and assist as needed.

(2) The initial or specialized response forces may be required to provide outer perimeter security as well as be prepared to manage the entire event. They must also be prepared to turn over responsibility for resolving the incident to HN security personnel if overseas or the FBI if within the United States and in the event the FBI seeks to exercise jurisdiction over the containment and resolution phases of the incident. These installation/base forces must always prepare for the most resource-demanding contingency. This level of readiness requires considerable sustainment training.

f. DOD installation military commanders and civilian managers have responsibility and authority for initial response, containment, and resolution of criminal incidents that occur on DOD facilities under their control prior to relinquishing that authority to the appropriate jurisdictional lead agency. In all cases, however, command of military elements remains within military channels. For detailed discussion on jurisdiction, authority, responsibilities, and other legal considerations concerning response to criminal incidents, see Chapter IV, "Legal Considerations," and Appendix K, "Jurisdictional Authority for Handling Terrorist Incidents."

4. Follow-On Response

The response to a terrorist incident varies depending on the nature and location of the incident. Generally there are four distinct phases through which an incident may evolve although many incidents do not develop beyond the first phase.

a. **Phase I: Locally Available Resources.** Phase I is the commitment of locally available incident response force (IRF) emergency first responders, and resources. Civilian contract guard services should not be used as part of an initial response force for a terrorist incident unless there is no federal law enforcement available. Civilian contract guard services should generally be restricted to perimeter security duties, traffic control, and crowd control activities. All initial responders, such as fire and medical personnel must understand and be trained to protect the incident location as a crime scene within established protocols. Ideally, ensure all LE or security personnel are familiar with local SOPs for terrorist incidents and have practiced these procedures

Basic firefighting and hazardous material response considerations should be integrated with incident and consequence management planning.

as part of their unit-training program. They must be prepared to secure, contain, and gather information at the scene until the beginning of Phase II. While securing and containing the incident scene, response forces must be alert to the fact terrorist incidents often include diversionary tactics and secondary attacks or devices with the desired purpose of harming first responder personnel. The evacuation or shelter-in-place of threatened areas is a high priority function.

b. **Phase II: Augmentation of Initial Response Force.** This phase begins when the EOC is activated. Phase II is the augmentation of the initial response force by additional emergency responder or specially trained response forces, such as special reaction team/emergency service team, FBI hostage rescue teams, HAZMAT/CBRNE containment teams, or HN units. On many installations, the IRF obtains its augmentation force from within or other personnel trained to augment the IRF. It's during this phase that the FBI or the HN may assume jurisdictional control over the incident. If that occurs, installation command and the incident commander must be ready to support the operation. Military assets will remain under the authority of the responsible military commander. The installation specially trained follow-on response forces must be ready for employment. Terrorist incidents conducted outside the continental US (OCONUS) against DOD installations, facilities, or units, the DOS and the US embassy play the key role in coordinating the USG and host country response.

c. **Phase III: Commitment of Counter-Terrorist Resources.** Phase III is the commitment of a specialized team from the FBI, DOD, USCG, or HN counter-terrorist force. In this phase, steps are taken to terminate the incident. Incident termination may be the result of successful negotiations, assault, or other actions, including the surrender or killing of the terrorists. Because

Proper planning includes common safety and mitigation considerations, such as adding fire breaks and protective measures between expeditionary shelters. Here SEAHUTs provide little protection or access during emergencies.

identifying the terrorists, as opposed to the hostages, may be difficult, it is important that the capturing forces handle and secure all initial captives as possible terrorists. The maritime environment provides additional factors for consideration in Phase III threat response. Due to the complexities of national and international boundaries, the challenges of the open ocean from the shore to the forward approaches, and the positioning of US response resources, the United States Navy and United States Coast Guard have both the support and response infrastructure to address most terrorist threats when other forces are either not available or outside their capability.

d. **Phase IV: Exploitation.** Critical to the success of CT operations is exploitation. Exploitation is the collection, analysis, and interrogation of materiel and personnel with the expectant result of gaining information and intelligence which will lead to additional AT and CT operations either regionally or globally. Exploitation is complementary and not to the exclusion of evidentiary requirements for prosecution of terrorists or their supporters.

5. Initial Response to a Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives Attack

a. Installations are required to establish an immediate response capability to ensure critical mission continuity and save lives during a CBRNE incident and to mitigate the situation in accordance with DODI 2000.18, *Department of Defense Installation Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive Emergency Response Guidelines*. National-level responders may not be immediately accessible or available to respond to an installation's

needs. Therefore, each installation must plan for the worst-case scenario by tailoring its response for each functional area, based on its organic resources and available local support through MOAs/MOUs. The situation may dictate that the installation not only conducts the initial response, but also sustains response operations.

b. In the event of a terrorist CBRNE incident, the commander should direct the following complementary sets of actions:

(1) Activate mass notification telling personnel to shelter in place, evacuate, or take other appropriate action.

(2) Activate the installation's initial response elements and local MOAs/MOUs.

(3) Initiate the DOD notification process.

(4) Request resources to augment the installation's response capabilities.

c. Installation commanders are responsible for ensuring their first responders have a plan and are equipped, trained, and exercised on the plan for responding to an incident involving CBRNE.

d. Installations are required to include incident response and CM measures in their AT plans. Use of the JAT Guide is an effective and approved method for developing a comprehensive AT plan that systematically addresses the spectrum of response considerations. The JAT Guide is further discussed in Appendix M, "Chemical, Biological, Radiological, and Nuclear Defense Planning Considerations," and is available online through www.atep.smil.mil or https://atep.dtic.mil/jatguide/. In the US, installation ATOs may want to consult with local fire/HAZMAT officials and the National Response Plan (NRP) to ensure complementary planning efforts.

Chemical, biological, radiological, or nuclear threats have diverse origins.

e. Terrorist CBRNE incidents, or threats of terrorist CBRNE acts, may overwhelm an installation's minimum capability to adequately detect, assess, or contain the threat. DOD, like most other local, state, or Federal entities, has neither the authority nor the expertise to respond unilaterally to all aspects of terrorist CBRNE threats or acts.

6. Special Considerations

See Figure VII-1.

a. **Establishing Communications.** A crucial aspect of implementing the AT plan is establishing secure communications among the forces in the incident area and the EOC. Once this is done, all other elements of the communications plan are activated. Communications personnel must be able to respond to changing needs during the incident and be able to maintain, over a prolonged period, the communications channels included in the AT plan.

b. **Evidence.** Although the primary goal is ending a terrorist incident without injury, another goal is the successful prosecution of terrorists. Witness testimony, photographic evidence, etc., are important in achieving a successful prosecution. Maintaining the continuous chain of custody on evidence obtained during an incident requires documenting the location, control, and possession of the evidence from the time custody is established until presenting the evidence in court. Failure to maintain the chain of custody can result in exclusion of the evidence. Consult LE or judge advocates on proper procedures unless doing so would harm military operations. Types of evidence for which the chain must be established include:

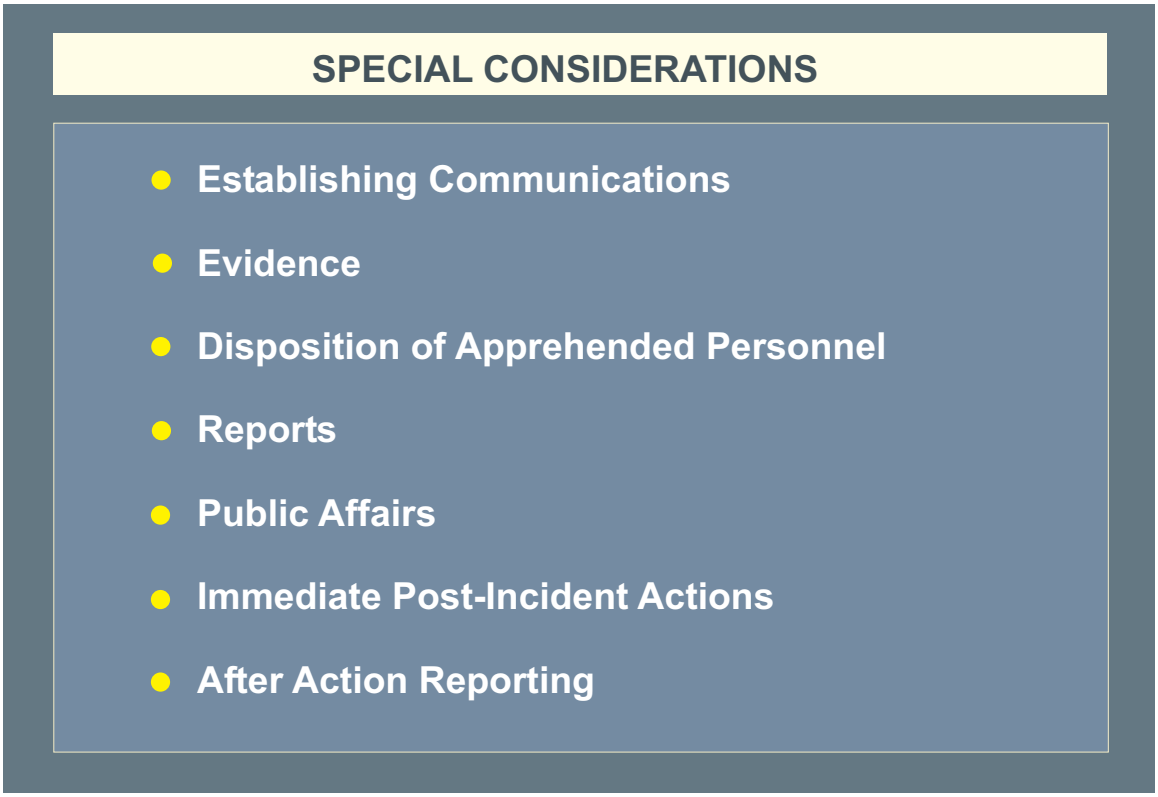


Figure VII-1. Special Considerations

(1) Photographs taken during the incident.

(2) Physical evidence, including any item(s) used by the terrorists. AT plans must include preplanning for contaminated evidence preservation, collection, storage, and chain of custody procedures.

(3) Tape recordings of conversations between terrorists and hostage negotiators.

(4) Demand notes or other messages recorded by written, audio, or video means prepared by the terrorists.

(5) Sample collection, including samples collected at the scene taken during initial and follow-on response.

c. **Disposition of Apprehended Personnel.** Apprehended military personnel must be handled according to the Uniform Code of Military Justice, DOD, and Service regulations and applicable installation SOPs. In the US, civilian detainees must be released to the FBI or US Federal marshals for disposition. In foreign incidents, civilian detainees may be processed according to the SOFA, diplomatic note, or other agreements with that particular country. Unless exigent circumstances dictate otherwise, the SJA should be consulted prior to releasing any individual to HN authorities. The United States does not, as a matter of policy, render its own nationals to the custody of a third party, including a HN. When this occurs, it does so only in very limited circumstances, and under the direction of the executive office. In coordination with the SJA, an after-action report should be prepared within seven working days after termination of the event.

d. **Reports.** Reporting to higher HQ is an important element in any special threat or terrorist situation. Each Service and command has a reporting procedure that requires a timely report of the incident to higher military authorities. The crisis management plan should dictate required reports and timelines for notification. This should include all staff journals and other documentation to include detailed information concerning disposition of evidence and captured individuals. The SJA and LE personnel should ensure this report is in sufficient detail to meet prosecution requirements.

e. **Public Affairs (PA).** Principal PA objectives of a terrorist incident crisis management plan are to ensure accurate information is provided to the public (including news media) and to communicate a calm, measured and reasonable reaction to the ongoing event.

(1) PA programs should attempt to:

(a) Identify terrorist activities as criminal acts not worthy of public support.

(b) Reiterate US policy on terrorism that identifies all terrorist acts as criminal acts, mandates no concessions to terrorists, refuses to pay ransom, and isolates those nations identified as encouraging, supporting or directing terrorism.

Bringing in medea representatives early under reasonable conditions maintains DOD credibility and preserves freedom of information.

(c) Support DOD PA strategy on releasing information pertaining to AT plans, operations, or forces involved in antiterrorist operations.

(2) The DOJ has lead PA responsibility for incidents occurring on US territory if the FBI assumes jurisdiction for resolving the incident. The Office of the Assistant Secretary of Defense (Public Affairs) (OASD (PA)) supports the DOJ in providing specific PA support.

(3) When US military forces are employed, DOD provides a spokesman for addressing military operational matters.

(4) The DOS coordinates PA during terrorist incidents overseas. The DOS may delegate the PA responsibility to a designated DOD representative.

(5) The OASD (PA) is the single point of contact for all PA aspects of US military AT actions. While there is no mandatory requirement to release information, installation commanders are advised to exercise prudent judgment on such matters and coordinate actions through PA channels to OASD (PA).

(6) When the EOC is activated, it should include the activities of the public affairs officer (PAO) and media center. The media center should be located in a separate location away from the EOC. The PAO shall prepare media releases and conduct briefings at the media center during the incident. The PAO shall use information obtained from EOC activities. The PAO shall ensure that all information is screened for intelligence information to maintain OPSEC. PA

shall coordinate with EOC personnel, and clear all information with the commander, prior to release. The PAO must be fully knowledgeable of the situation as it develops. The media representatives should not have direct access to hostages, hostage takers, communications nets, or anyone directly involved in a terrorist incident unless the PAO has cleared such contact with the EOC. DOD experience with media representatives has shown that bringing them in early under reasonable conditions and restrictions commensurate with the risk and gravity of the event, and providing them thorough briefings, maintains DOD credibility and preserves freedom of information.

f. **Immediate Post-Incident Actions.** During the immediate post-incident phase, medical, psychological, and chaplain attention, along with other support services, should be given to all personnel involved in the operation, including captured terrorists. Critical incident stress debriefing (CISD) is a regular element of civilian first responder activities. Additional CISD information is available at www.icisf.org. Contact the chaplains office for additional Service guidance and support. A final briefing should be given to media personnel; however, they should not be permitted to visit the incident site until the investigation is complete and such access is cleared by appropriate officials. Because of the criminal nature of the terrorist event, the site must be secured until the crime scene investigation is completed by the appropriate investigative agency. It is also imperative to record every action that occurred during the incident.

g. **After Action Reporting.** Conducting comprehensive reviews after an incident is as critical as conducting reviews or lessons learned evaluations after an exercise. Information from all levels of the command concerning positive, negative, and neutral factors that contributed to the incident and its resolution should be analyzed to determine elements of installation or unit plans that should be changed. Interagency or local officials involved in the activity should also be engaged to determine their perspective. Once compiled, after action reports or lessons learned should be shared with other units and defense components. As outlined in Chapter II, "Terrorist Threat," terrorists continue to refine their tactics and actively conduct surveillance to identify vulnerabilities in friendly TTPs. After action reports, whether for real incidents or exercises, are one mechanism for improving friendly capabilities and remaining ahead of the terrorist.

7. Considerations in the United States

The following information is included as a reference for DOD commanders, and is especially relevant for DOD installations located in the US or US territories. In the US, AT, natural disaster, and other 'all hazard' planning and response efforts will integrate NRP and NIMS principles as necessary because of the mutual interdependencies with local emergency management operations.

a. US National Incident Response

(1) Since the tragic events of September 11, 2001, the United States has resolved to better prepare to prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism, major disasters, and other emergencies; and minimize the damage and recover from attacks, major disasters, and other emergencies that occur. These complex and emerging

21st century threats and hazards demand a unified and coordinated national approach to domestic incident management.

(2) The NRP specifies how the resources of the Federal government will work in concert with state, local, and tribal governments and the private sector to respond to incidents of national significance. The NRP is predicated on the NIMS. Together, the NRP and the NIMS provide a nationwide template for working together to prevent or respond to threats and incidents regardless of cause, size, or complexity.

(3) The NRP establishes a comprehensive all-hazards approach to enhance the ability of the US to manage domestic incidents. The plan incorporates best practices and procedures from incident management disciplines — homeland security, emergency management, law enforcement, firefighting, public works, public health, responder and recovery worker health and safety, emergency medical services, and the private sector — and integrates them into a unified structure. It forms the basis of how the Federal government coordinates with state, local, and tribal governments and the private sector during incidents. It establishes protocols to help:

(a) Save lives and protect the health and safety of the public, responders, and recovery workers.

(b) Ensure security of the homeland.

(c) Prevent an imminent incident, including acts of terrorism, from occurring.

(d) Protect and restore critical infrastructure and key resources.

(e) Conduct LE investigations to resolve the incident, apprehend the perpetrators, and collect and preserve evidence for prosecution and/or attribution.

(f) Protect property and mitigate damages and impacts to individuals, communities, and the environment.

(g) Facilitate recovery of individuals, families, businesses, governments, and the environment.

The NRP is available at http://www.dhs.gov/dhspublic/interweb/assetlibrary/NRPbaseplan.pdf.

b. **National Incident Management System**

(1) NIMS provides a consistent nationwide template to enable all government, private-sector, and nongovernmental organizations to work together during domestic incidents.

(2) Developed by the Secretary of Homeland Security at the request of the President, NIMS integrates effective practices in emergency preparedness and response into a comprehensive

national framework for incident management. The NIMS will enable responders at all levels to work together more effectively to manage domestic incidents no matter what the cause, size or complexity. NIMS is a comprehensive, national approach to incident management that is applicable at all jurisdictional levels and across functional disciplines. The intent of NIMS is to:

(a) Be applicable across a full spectrum of potential incidents and hazard scenarios, regardless of size or complexity.

(b) Improve coordination and cooperation between public and private entities in a variety of domestic incident management activities.

(c) Provide a framework for interoperability and compatibility by balancing flexibility and standardization.

(3) The benefits of the NIMS system include the following:

(a) Standardized organizational structures, processes and procedures.

(b) Standards for planning, training and exercising, and personnel qualification.

(c) Equipment acquisition and certification standards.

(d) Interoperable communications processes, procedures, and systems.

(e) Information management systems.

(f) Supporting technologies — voice and data communications systems, information systems, data display systems, and specialized technologies.

c. **NIMS Command and Management**

(1) NIMS standard incident management structures are based on three key organizational systems:

(a) The **ICS**, which defines the operating characteristics, management components, and structure of incident management organizations throughout the life cycle of an incident.

1. The **ICS** is a proven on-scene, all-hazard incident management concept. ICS has become the standard for on-scene management.

2. ICS is interdisciplinary and organizationally flexible to meet the needs of incidents of any size or level of complexity.

3. ICS has been used for a wide range of incidents—from planned events to HAZMAT spills to acts of terrorism.

(b) **Multiagency Coordination Systems**, which define the operating characteristics, management components, and organizational structures of supporting entities.

(c) **Public Information Systems**, which include the processes, procedures, and systems for communicating timely and accurate information to the public during emergency situations.

(2) **Preparedness.** Similar to the DOD AT program, NIMS concludes that effective incident management begins with a host of preparedness activities. These preparedness efforts are conducted on a "steady-state" basis, well in advance of any potential incident. According to NIMS, preparedness involves a combination of:

(a) Planning, training, and exercises.

(b) Personnel qualification and certification standards.

(c) Equipment acquisition and certification standards.

(d) Publication management processes and activities.

(e) Mutual aid agreements.

(f) Emergency Management Assistance Compacts.

Additional information about NIMS is available at http://www.fema.gov/nims/.

APPENDIX A
CRITICALITY ASSESSMENT

1. General

This appendix describes the methodology commanders and civilian equivalents can use to complete a criticality assessment. A critical asset is a specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation to continue to function effectively. Both regulations and the commander's priorities and intent determine critical assets. Regulations cover items such as very important persons, ammunition storage areas, etc. The commander's intent extends coverage to other items such as mission critical and high occupancy assets. Critical assets can be people, property, equipment, activities and operations, information, facilities, and materials as well as the interdependent networks that connect many of them.

2. Conducting the Criticality Assessment

a. The criticality assessment identifies assets supporting DOD missions, units, or activities and deemed critical by military commanders or civilian agency managers. For AT purposes, the criticality assessment should include high-population facilities, which may not necessarily be mission essential (recreational activities, theaters, or sports venues). It addresses the impact of temporary or permanent loss of assets. It examines costs of recovery and reconstitution including time, dollars, capability, and infrastructure support.

b. In military units deployed under the command of the Services or a combatant command, the staff at each command echelon determines and prioritizes critical assets. The commander responsible for AT approves the prioritized list. The criticality assessment goals are:

(1) Identify installation's/unit's key assets.

(2) Determine whether critical functions can be duplicated under various attack scenarios.

(3) Determine time required to duplicate key assets or infrastructures efforts if temporarily or permanently lost.

(4) Determine priority of response to key assets, functions, and infrastructures in the event of fire, multiple bombings, or other terrorist acts.

c. The assessment process described below is specifically designed for AT assessment and planning. Other DOD processes, such as MEVA, the mission, symbolism, history, accessibility, recognizability, population, and proximity (MSHARPP) methodology, and the criticality, accessibility, recuperability, vulnerability, effect, and recognizability (CARVER) matrix tool, offer similar types of subjective assessments but are not specifically tailored for AT assessments. While the MSHARPP and CARVER processes are optional methodologies for those who are

familiar with their use, both have design limitations and are best used only as an adjunct to the risk assessment (combination of the criticality, threat, and vulnerability assessment ratings) and management methodology.

d. The purpose of the criticality assessment process is to identify and prioritize all assets on an installation. Assets include personnel, equipment, stockpiles, buildings, or transportation systems that are deemed critical as defined by DODD 3020.40, *Defense Critical Infrastructure Program*. There are many different types of assets critical to mission accomplishment and it is important not to exclude some assets because they are not necessarily mission-essential or physically located on the installation. For example, a telephone switching facility located off base may be essential to communications if alternative systems are not identified. There may also be assets on the installation which are not critical to the direct operation of the installation, but are critical to DOD.

e. It may also be useful to link identified threat attack means to a specific time period or location. For example, a terrorist group operating in the proximity of the installation may typically target areas, such as schools or the commissary and/or exchange that contain a large number of people at certain times.

f. When determining asset criticality, use of the following criteria shall assist in standardizing the process.

(1) Importance. Measures the value of the area or assets located in the area, considering their function, inherent nature, and monetary value.

(2) Effect. Measures the ramification of a terrorist incident in the area, considering the psychological, economic, sociological, and military impacts.

(3) Recoverability. Measures the time required for the function occurring at that area to be restored, considering the availability of resources, parts, expertise and manpower, and redundancies. Even if a DOD asset is injured, damaged, or destroyed, it may have future value in the accomplishment of other DOD missions or be of great symbolic value to DOD, the US government, and the American people. Consideration should therefore be given to the resources that must be expended to recover an asset and in some cases, repair it for return to service with DOD in the future.

(4) Mission Functionality. Measures key positions, special facilities, specialized equipment, etc., used to fulfill assigned missions.

(5) Substitutability. Are there substitutes available for personnel, facilities or materiel? Can assigned missions be performed using substitutes? If the substitutes are less capable, can the mission still be accomplished successfully?

(6) Repairability. If a DOD asset is injured or damaged, can it be repaired and rendered operable? How much would it cost? Could repairs be accomplished in a timely manner? Would

repairs degrade asset performance, and if so, can the mission be accomplished in the degraded condition?

3. Suggested Methodologies

a. Installation commanders are encouraged to use a risk assessment tool that is simple yet has some quantifiable logic to help in decision making. Assessment teams shall use the methodology to determine terrorist options against specific targets and use them as examples of protection strategies discussed in this appendix. The suggested tools each have their strengths and weaknesses with regard to their applicability to a particular threat situation. Use the tool most appropriate to your particular environment. As an example, CARVER is not specifically tailored for AT assessments, although it can be used. Likewise, MSHARPP is a targeting analysis tool geared more closely to assessing personnel vulnerabilities. Assessment team members should be cognizant of potential gaps when choosing one methodology over another. The use of the Joint Staff CVAMP shall assist commanders and ATOs in managing their command's vulnerabilities and associated funding requirements.

b. MSHARPP

(1) The purpose of the MSHARPP matrix is to analyze likely terrorist targets. Consideration is given to the local threat, likely means of attack available to the enemy, and variables affecting the disposition (e.g., "attractiveness" to enemy, potential psychological effect on community) of potential targets. This section provides an example of how to use MSHARPP.

(2) After developing a list of potential targets, use the MSHARPP selection factors to assist in further refining your assessment by associating a weapon/tactic to a potential target to determine the efficiency, effectiveness, and plausibility of the method of attack and to identify vulnerabilities related to the target. After the MSHARPP values for each target or component are assigned, the sum of the values indicates the highest value target (for a particular mode of attack) within the limits of the enemy's known capabilities.

(3) Mission. Mission focuses mainly on the threat to the situations, activities, capabilities, and resources on an installation that are vulnerable to a terrorist attack. The mission components consist of the equipment, information, facilities, and/or operations or activities that are necessary to accomplish the installation's mission.

(a) When assessing points in this area, determine whether or not an attack on mission components shall cause degradation by assessing the component's:

1. Importance. Importance measures the value of the area or assets located in the area, considering their function, inherent nature, and monetary value.

2. Effect. Effect measures the ramifications of a terrorist incident in the area, considering the psychological, economic, sociological, and military impacts.

3. Recuperability. Recuperability measures the time required for the function occurring at that area to be restored, considering the availability of resources, parts, expertise and manpower, and redundancies.

(b) Mission Criteria Scale. Assess points to the target equipment, information, facilities, and/or operations or activities (scale of 1-5; 5 being worst) in this area based upon the degree of mission degradation if attacked by a terrorist.

1. ONE. Destroying or disrupting this asset would have no effect on the ability of the installation to accomplish its mission.

2. TWO. The installation could continue to carry out its mission if this asset were attacked, albeit with some degradation in effectiveness.

3. THREE. Half of the mission capability remains if the asset were successfully attacked.

4. FOUR. Ability to carry out a primary mission of the installation would be significantly impaired if this asset were successfully attacked.

5. FIVE. Installation cannot continue to carry out its mission until the attacked asset is restored.

(4) Symbolism. Consider whether the target represents, or is perceived by the enemy to represent, a symbol of a targeted group (e.g., symbolic of US military, religion, government, authority). Assess points in this area based upon the symbolic value of the target to the enemy. Symbolism criteria scale:

(a) ONE. Low profile or obscure symbol, demonstrates no strength or capability not common knowledge.

(b) TWO. Low profile, direct symbol, local publicity, demonstrates no new capability or willingness.

(c) THREE. Symbolic, achieves limited global publicity, demonstrates no new capability or willingness.

(d) FOUR. Prominent symbol, global publicity, demonstrates previously unconfirmed capability or willingness.

(e) FIVE. High profile, direct symbol, sustained global publicity, demonstrates previously unknown capability or willingness

(5) History. Do terrorist groups have a history of attacking this type of target? While you must consider terrorist trends worldwide, focus on local targeting history and capabilities. History criteria scale:

(a) ONE. Little or no history of attacking this type of asset.

(b) TWO. Difficult to recognize under any condition, requires training for recognition; limited open source information, architecture, or signage exists.

(c) THREE. Recent, credible threats against this type of asset.

(d) FOUR. Historically common target, attacks against this asset has occurred in the past, general threat against this type of asset.

(e) FIVE. Favored target, recent attacks within the local geographic area, credible threat against this type of asset.

(6) Accessibility. A target is accessible when an operational element can reach the target with sufficient personnel and equipment to accomplish its mission. A target can be accessible even if it requires the assistance of knowledgeable insiders. This assessment entails identifying and studying critical paths that the operational element must take to achieve its objectives, and measuring those things that aid or impede access. The enemy must not only be able to reach the target but must also remain there for an extended period.

(a) ONE. Not accessible without extreme difficulty; attempted surveillance is extremely difficult or easily detected.

(b) TWO. Protected perimeter, defense in depth and detection capability; Not easily surveilled, few hostile surveillance locations and little open source information exist, perimeter penetration required.

(c) THREE. Protected perimeter, limited defense in depth and detection capability; Easily surveilled, hostile surveillance locations and open source information exist.

(d) FOUR. Limited perimeter protection, defense in depth and detection capability; Easily surveilled, multiple hostile surveillance locations and open source information.

(e) FIVE. No perimeter protection, defense in depth, or detection capability; surveillance can be conducted "at will."

(7) Recognizability. A target's recognizability is the degree to which it can be recognized by an operational element and/or intelligence collection and reconnaissance asset under varying conditions. Weather has an obvious and significant impact on visibility (friendly and enemy). Rain, snow, and ground fog may obscure observation. Road segments with sparse vegetation and adjacent high ground provide excellent conditions for good observation. Distance, light,

and season must be considered. Other factors that influence recognizability include the size and complexity of the target, the existence of distinctive target signatures, the presence of masking or camouflage, and the technical sophistication and training of the enemy. Recognizability criteria scale:

(a) ONE. Cannot be recognized under any conditions — except by experts; little useful or no open source information, architecture, or signage exists.

(b) TWO. Difficult to recognize under any condition, requires training for recognition; limited open source information, architecture, or signage exists.

(c) THREE. Difficult to recognize at night or in bad weather, or might be confused with other targets; requires training for recognition; limited open source information, architecture, or signage exists.

(d) FOUR. Easily recognizable and requires a small amount of training for recognition; some open source information, architecture, or signage serve to reveal the nature of the asset.

(8) Population. Population addresses two factors: quantity of personnel and their demography. Demography asks the question "who are the targets?" Depending on the ideology of the terrorist group(s), being a member of a particular demographic group can make someone (or some group) a more likely target.

(a) ONE. No people present or infrequently populated by very few people; contains people that the terrorist group considers desirable to avoid harming.

(b) TWO. Sparsely populated; prone to having small groups or individuals, little target value based on demographics of occupants.

(c) THREE. Moderate number of people, known target group may be present; no special segment necessary for mission accomplishment.

(9) Proximity. Is the potential target located near other personnel, facilities, or resources that, because of their intrinsic value or "protected" status and a fear of collateral damage, afford it some form of protection? (e.g., near national monuments, protected/religious symbols that the enemy holds in high regard).

(a) ONE. Asset is adjacent to assets that are undesirable to attack or damage.

(b) TWO. Asset is isolated, no access to other assets.

(c) THREE. Asset is isolated; however, access to this asset would allow access to other assets.

(10) In an MSHARPP worksheet, values from 1 to 5 are assigned to each factor based on the associated data for each target. Five represents the highest vulnerability or likelihood of attack and 1 the lowest. Accordingly, the higher the total score, the more vulnerable the target. Because this analysis is highly subjective, some analysts prefer simple "stoplight" charts with red, yellow and green markers representing descending degrees of vulnerability. The MSHARPP analysis must consider both the present FP posture and enhanced postures proposed for escalating FPCONs. Specific target vulnerabilities must be combined with exploitable perimeter control vulnerabilities. If access routes are well protected and not deemed exploitable an otherwise vulnerable building becomes a less likely target.

c. CARVER

(1) CARVER is a very useful tool for determining that your critical assets might indeed offer an enemy a good or soft target. If you employ the very same CARVER analysis to every asset, it shall yield a good estimate as to the attractiveness of those assets to an enemy. Specifically commanders shall then know which "targets" require hardening or otherwise increased protection.

(2) The acronym CARVER represents the following:

(a) Criticality. The importance of a system, subsystem, complex, or component. A target is critical when its destruction or damage has a significant impact on the output of the targeted system, subsystem, or complex, and at the highest level, on the unit's ability to make war or perform essential functions. Criticality depends on several factors:

1. How rapidly shall the impact of asset destruction affect the unit's essential functions?

2. What percentage of output and essential functions is curtailed by asset damage?

3. Is there an existence of substitutes for the output product or service?

4. What is the number of assets and their position in the system or complex flow diagram?

5. Criticality asks the question: How critical is the asset to your mission accomplishment?

(b) Accessibility. The ease that an asset can be reached, either physically or by standoff weapons. An asset is accessible when a terrorist element can physically infiltrate the asset, or the asset can be hit by direct or indirect fire. As a reminder, assets can be people, places, or things. The use of standoff weapons should always be considered when evaluating accessibility. Survivability of the attacker is usually most related to a target's accessibility. Accessibility asks the question: How easily can an enemy get access to, or have their weapons reach the asset?

(c) Recuperability. A measure of time required to replace, repair, or bypass, the destruction or damage inflicted on the target. Recuperability varies with the sources and ages of targeted components and with the availability of spare parts. The existence of economic embargoes and the technical resources of the installation shall influence recuperability. Recuperability asks the question: How long would it take you to repair or replace the asset?

(d) Vulnerability. A measure of the ability of the terrorist to damage the target using available assets (people and material). A target (asset) is vulnerable if the terrorist has the means and expertise to successfully attack it. Vulnerability depends on:

1. The nature of the construction of the target.

2. The assets available (manpower, transportation, weapons, explosives, and equipment) to defend the asset.

3. Vulnerability asks the questions: Is the asset literally hardened or guarded? Are measures in place to mitigate any threat?

(e) Effect on the population. The positive or negative influence on the population as a result of the action taken. Effect not only considers the public reaction in the vicinity of the target, but also considers the domestic and international reaction as well. Will reprisals against friendlies result? Will national psychological operations (PSYOP) themes be contradicted or reinforced? Will exfiltration and evasion be helped or hurt? Will the enemy population be alienated from its government, or shall it become supportive of the government? Effect is often neutral at the tactical level. Effect asks the question: What is the effect on the local population, be it terror or demoralization, and associated mission degradation?

(f) Recognizability. The degree that a target can be recognized under varying weather, light, and seasonal conditions without confusion with other targets or components.

1. Factors that influence recognizability include the size and complexity of the target, the existence of distinctive target signatures, and the technical sophistication and training of the terrorists.

2. Recognizability asks the question: Can the enemy recognize the target for what it truly is and its importance?

(3) Target selection requires detailed intelligence and thorough planning, and is based on the CARVER factors identified above. The CARVER matrix is a decision tool for rating the relative desirability of potential targets and for wisely allocating attack resources. Two rules of thumb apply for completing the matrix:

(a) For strategic level analysis, list systems and subsystems.

(b) For tactical level analysis list complexes or components of subsystems and complexes. Keep in mind that the scale can be adjusted, such as one to ten or 10 to 100, provided that consistency is observed.

(4) After completing the matrix for all assets, total the scores and then rank order those totals to prioritize vulnerabilities.

(5) The following are basic mitigation tips to address four of the six CARVER components:

(a) Reduce criticality. As practicable have a back-up device, system, or tested plan to afford mission accomplishment without the asset; create redundancy either physically or operationally; have a tested and viable COOP plan; and have a fall-back site for conducting the same mission from another location.

(b) Reduce accessibility. Reduce access, both physical and cyber, as applicable; use barriers, other barricades, carefully controlled pedestrian and vehicle movement and/or access and parking; and use fences, remote motion sensors, and remote video surveillance.

(c) Reduce vulnerability. Harden the structure and/or immediate environment to include window treatment to prevent glass shards, structural reinforcement, and shatterproof and fireproof building materials. Move vehicle parking and access sufficiently away from personnel massing facilities.

(d) Reduce recognizability. Delete location and purpose of facility from all base maps and remove building signs that describe function or give title of unit in facility. Instruct telephone operators to not give out number or existence of facility. Use plant cover, including trees and bushes, to partially conceal facility, particularly from roads.

4. Criticality Assessment Matrix

a. The purpose of a criticality assessment matrix is to determine the criticality of each asset, which shall also help to prioritize them. For each asset, the assessment team shall assign values for each criteria based on a scale, such as one to ten. The assessment team must determine what criteria to use.

b. Once all asset values are tallied, they can be rank-ordered such that highest score is "most critical" and lowest score is "least critical." However, it is important to emphasize that not all assets in the matrix shall be "essential for mission accomplishment".

Intentionally Blank

APPENDIX B
THREAT ASSESSMENT

1. Introduction and Overview

The risk management process begins with an assessment of the terrorist threat to DOD personnel and facilities. The AT TA is used to identify the terrorist threats posed to DOD assets and/or the threats that could be encountered in executing a mission.

2. Threat Assessment

a. The TA system is vital to developing and disseminating terrorism warnings. Specific warning information — time, date, place, those involved, and method of attack — is rarely voluntarily provided by terrorists. Careful threat analysis is required to detect and correctly evaluate pre-incident indicators of a terrorist attack, so timely warning messages can be issued.

b. Threat analysis provides the intelligence officer with information upon which to base warnings.

c. Threat information for AT programs is diverse and includes foreign intelligence, open source materials, domestic criminal information, and information from Federal, state, and local governments.

d. A standardized format for the Defense Threat Assessment (DTA) has been promulgated by the Office of the Undersecretary of Defense, Counterintelligence and Security that should be used when preparing local TAs. The Defense Threat Assessment Tool, developed by the Joint Counterintelligence Training Academy provides guidance on completing the DTA.

e. Defense terrorism awareness messages (DTAMs) summarize recent, credible threat reporting concerning DOD or US interests. Messages are issued when specificity of timing or target cannot be ascertained. DTAMs do not expire but can become dated.

3. Installation Level Antiterrorism Threat Assessment Requirements and Activities

a. Commanders down to the installation or tenant level task the appropriate organizations under their command to gather, analyze, and disseminate terrorism threat information or receive these services from the CI organization assigned to support them. When organic intelligence/counterintelligence/law enforcement assets are not available, commanders should request support from higher authority. The full range of intelligence, CI, and LE capabilities shall be utilized in support of distinct and separate TA requirements: annual TAs and ongoing assessment of the local threat.

b. **Annual Threat Assessment.** Installation commanders shall, at least annually, prepare a terrorism TA for those personnel and assets for which they have AT responsibilities. Whereas

DOD Threat Methodology focuses on the degree of activity of known terrorist groups, the annual TA seeks to identify the full range of feasible terrorist capabilities (weapons, tactics, techniques, and methods of attack) that could reasonably be used against the installation or its personnel. Even in the absence of a current known threat group, an assessment is a necessary input to the required annual VA and for planning physical and procedural countermeasures. Annual TAs should include all likely or feasible WMD including CBRNE threats.

c. **Threat Matrix.** Although not required, one tool that may assist in the preparation of the TA and AT plan is the threat matrix. Preparation of the annual TA requires careful analysis of known local threats, together with estimates of relevant national and transnational threat capabilities. Locally derived, open-source information regarding the availability of weapons and component materials in the area is also necessary in developing the range of threats. Threat analysts preparing the assessment should differentiate threats likely to be used inside the perimeter from those more likely to be used outside the perimeter to aid in the VA and development of countermeasures. The threat matrix unambiguously establishes the range of specific threat capabilities that shall be used to analyze vulnerabilities and plan countermeasures. The threat matrix is a planning tool which ensures that security and procedural countermeasures are economically designed to counter specific threats or mitigate specific vulnerabilities, and that the risk remaining is well understood by commanders making risk acceptance decisions.

d. Both installation and unit commanders shall assess the terrorist threat for probability and severity of occurrence. Probability is the estimate of the likelihood that a threat shall cause an impact on the mission or a hazard to the installation. Severity is an estimate of the threat in terms of the degree of injury, property damage, or other mission-impairing factors. By combining estimates of severity and probability, an assessment of risk can be made for each threat. A matrix may be used to assist in identifying the level of risk. The outcome of this process is a prioritized list of threats. The highest priority threat is the one that poses the most serious risk in terms of likelihood and severity. This list of prioritized threats shall be used to evaluate the acceptability of certain risks and which risks for which to make decisions concerning the employment of resources and other actions that reduce vulnerability. This assessment should be recorded as a record/baseline and updated regularly as the threat changes. Services and combatant commanders may develop separate, more complete methodologies for assessment. If installation and unit commanders do not have the resources to assess the threat for probability and severity of occurrence, they should coordinate with their next higher echelon to assist with this requirement.

e. TAs of specific operations, missions or events may also be conducted to identify specific threats to the conduct of those activities.

f. In addition to preparing an annual TA, commanders must also continuously assess local threat information so appropriate FPCONs can be set. Commanders at all levels shall forward up and down the chain of command all information pertaining to suspected terrorist threats, or acts of terrorism involving DOD personnel or assets for which they have AT responsibility. Threat information shall be used in the determination to raise or lower the present FPCON.

Continuous threat analysis also supports the warning of suspected target facilities or personnel through the installation's mass notification system when the information relates threats of an immediate nature.

Intentionally Blank

APPENDIX C
VULNERABILITY ASSESSMENT

1. General

A VA is the process the commander uses to determine the susceptibility of assets to attack from threats identified by the AT TA. The VA answers the question "what kind of attack is the asset most/least vulnerable to?" DODI 2000.16, *DOD Antiterrorism Standards*, provides authoritative standards regarding both installation and deploying unit VAs. Vulnerabilities exist at every installation as a result of the terrorist threat faced. Vulnerabilities are always there, no matter the policies, procedures, structures, and protective equipment. Although terrorist threats cannot be controlled, they can be assessed and the vulnerability of assets to those threats can be mitigated. Identifying and understanding vulnerabilities are important in determining how well an asset shall be protected from loss. Vulnerabilities are also the component of overall risk over which the commander has the most control and greatest influence. By reducing vulnerability, the potential risk to an asset is also reduced.

2. Assessing Vulnerability

a. Installation or unit AT officers conduct a VA using key AT working group members in a collaborative effort as the assessment team. Teams should include representation from operations, security, intelligence, counterintelligence, law enforcement, communications, fire department, engineers, medical services, housing, emergency planning, and WMD planning and response. The VA must be conducted in accordance with DODI 2000.16, *DOD Antiterrorism Standards*, and DODI 2000.18, *DOD Installation Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive Emergency Response Guidelines*.

b. The end-state of the VA process is the identification of physical characteristics or procedures that render critical assets, areas, or special events vulnerable to a range of known or feasible terrorist capabilities. Determination of vulnerability is partly a function of the commander's desired level of protection for the asset, area, or special event. Although performing a detailed VA is not simple, the results quantifying and rating the effectiveness of an installation's current protective measures are invaluable and provide a major tool for developing AT countermeasures. The VA methodology should follow the below sequence:

(1) List assets and the threats against those assets.

(2) Determine criteria to be used to assess assets against.

(3) Train assessment team on assessment intent and methodology.

(4) Assessment team conducts assessment.

(5) Consolidate and review assessment results.

c. The DOD has created several tools to perform criticality assessment to support the VA process to include the mission, symbolism, history, accessibility, recognizability, population, and proximity (MSHARPP); and criticality, accessibility, recuperability, vulnerability, effect, and recognizability (CARVER). The DTRA AT VA Team Guidelines are another excellent tool available for local (base) VAs. This is a comprehensive checklist that is directly linked to DODI 2000.16, *DOD Antiterrorism Standards*, and produces a product similar to a Joint Staff Integrated VA (JSIVA). The JAT Guide also assists commanders in AT planning and risk management. It is further explained in Appendix N, "Joint Antiterrorism Program Manager's Guide." It can be accessed through http://www.atep.smil.mil.

d. Core Vulnerability Assessment Management Program

(1) CVAMP is an automated and web-based means of managing a command's vulnerabilities and associated funding requirements. CVAMP key capabilities include:

(a) Provide a means to enter VA findings into a database in accordance with DODI 2000.16, *DOD Antiterrorism Standards*, for both higher headquarters and local assessments.

(b) Provide capability of receiving observations directly from the JSIVA Information System.

(c) Document a commander's risk assessment decision for each vulnerability.

(d) Track the status of known vulnerabilities until mitigated.

(e) Provide a tool to assist in prioritizing vulnerabilities via a weighted scale based on user input.

(f) Provide commanders a vehicle to identify requirements to the responsible chain of command.

(g) Provide the ability to roll vulnerability data into a resource requirement. This includes unfunded requirement (UFR) submissions as well as emergent and emergency CbT-RIF requests. Use of CVAMP is mandatory for submission to the Joint Staff of CbT-RIF requests.

(h) Provide ability to control release of vulnerabilities and associated funding requests through the chain of command — access is limited to a "need to know" basis as determined by system administrators at each command level.

(i) Allow for prioritization of emergent CbT-RIF requests and UFRs as well as provide a tool to assist in this process based on user input.

(j) Provide a ready reference to track the status of installations and activities by FPCON and/or terrorism threat level.

(2) Registration for CVAMP is embedded within the Joint Staff's Antiterrorism Enterprise Portal via the SECRET Internet Protocol Router Network (SIPRNET). Once registered on ATEP, system administrators identified at each level of command shall assign CVAMP roles and functions to users based on their needs/requirements. To allow for flexibility, administrators can assign multiple roles to a user. Each role sets specific user permissions within the system. Besides SIPRNET access, minimal additional equipment is required to use CVAMP. The system operates in a user-friendly format with drop down menus and no complex computer skills are required to create, review, modify or manage the program. Initial CVAMP-related roles and their permissions are:

(a) Commander. Capability to read and/or write with comment and retains sole release authority to higher headquarters on all vulnerability assessments, vulnerabilities, and funding requests.

(b) ATO. Capability to create vulnerability assessments, vulnerabilities and funding requests.

(c) Resource Manager. Capability to read and/or write to all funding requests.

(d) Assessor. Capability to create observations associated with a vulnerability assessment.

(e) System Administrator. Capability to assign and manage roles within immediate organization and one level down.

(f) Users should contact their local/and or next higher headquarters CVAMP administrators to establish their roles within CVAMP.

Intentionally Blank

APPENDIX D
RISK ASSESSMENT

1. Introduction

As discussed in Chapter V, "Antiterrorism Program: Installation, Base, Ship, Unit, and Port," the risk assessment (RA) combines criticality, threat, and vulnerability assessments in order to provide a more complete picture of the risks to an asset or group of assets. This appendix describes the methodology commanders and civilian equivalents can use to assess risk.

2. Risk Assessment Methodology

a. The RA is a logical, step-by-step method, and shall require the participation of the entire staff. In starting the RA process, commanders should examine three elements: threat, criticality, and vulnerability.

(1) **Threat.** The threat is determined through a proper and thorough TA. The TA should identify the likelihood and severity of the terrorist to inflict injury to a person or damage to a facility or asset by considering terrorist capability, intent, and objectives. To enable commanders to focus their analysis, the TA should also specify the type of weapon(s) or act(s) the terrorist shall use to initiate the event (assassination, bomb, etc.).

(2) **Asset Criticality.** Critical assets are determined by both the term and the measure of importance to the installation's mission. Areas that encompass multiple critical assets are referred to as critical areas. The criticality assessment provides information to prioritize assets and allocate resources to special protective actions.

(3) **Vulnerability.** A thorough VA shall highlight the susceptibility of a person, group, unit, facility, or asset to a damaging incident. VAs should also address the capabilities of response elements to plan those activities that support the installation's ability to either deter and/or respond to terrorist threats and incidents. For example, a VA might reveal weaknesses in an organization's security systems, financial management processes, computer networks, or unprotected key infrastructure such as water supplies, bridges, and tunnels. There may be several vulnerability assessments conducted on an installation (e.g., water vulnerability, CBRNE vulnerability); the findings of these functional area vulnerability assessments must be included in the overall installation assessment.

b. During the RA process, the commander must consider all of the aforementioned elements, to make well-informed decisions when planning FPCON measure implementation, and terrorist incident response measures. The RA and management process described here does not dictate how to conduct the assessment, nor does it discuss how to identify deficiencies and vulnerabilities. It outlines what type of information to collect and how to organize and display that information for decision making. If the installation does not have the resident expertise to conduct an AT RA, consider using a JSIVA, and/or combatant commander or Service AT assessment reports.

Vulnerabilities and deficiencies gathered from these useful reports can be plugged directly into the methodology outlined in this appendix.

c. Given the resource-constrained environment in which installations now operate, installation commanders or their civilian equivalents require a method to assist them in making resource allocation decisions to protect the installation from possible terrorist threats (FPCON measure implementation and other mitigation efforts) and to most effectively respond should a terrorist incident occur (response measures). Risk management is the process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk costs with mission benefits. The risk management process allows installation commanders to use representative (operational) risk as one of the principal factors in their decision-making process. In this context, representative risk shows the relative impact on an installation's assets, given a stated attack. Representative risk is NOT a prediction that a terrorist incident shall occur.

d. The example below shall focus on vulnerabilities of critical assets. This same methodology can be applied to other areas of interest such as response capability. It is also important to emphasize that this methodology is merely a tool to assist commanders and civilian equivalents in assessing and managing risk.

3. Assessing Risk — A Practical Exercise

a. This example presumes that a commander has completed the threat, criticality, and VAs. The process begins by creating an asset RA table. In addition to isolated assets, areas can be assessed in terms of the criticality of the assets located within it and its vulnerability to specific threats. The installation assessment team shall rate each asset for every type of threat identified in the TA.

b. To complete the RA table, begin by determining the asset to be examined. Create and label the row with the asset and label each column as illustrated in Figure D-1.

(1) **Attack Means.** Method by which the asset would be attacked. Different groups may present several different attack methods based on what weapons they possess and the methods they use. Sample attack means include small arms fire, car/truck bomb, chemical weapons, biological weapons, etc. Use the information from Chapter V, "Antiterrorism Program: Installation, Base, Ship, Unit, and Port."

(2) **Criticality.** Obtained from the information gathered in Chapter VI, "Preventive Measures and Considerations."

(3) **Vulnerability.** Obtained from the information gathered in Chapter VII, "Incident Response and Consequence Management."

c. An Example. Consider a command post located in a building on a military installation. The building is constructed of 12 inch concrete walls, has no windows and the ventilation system

EXAMPLE ASSET RISK ASSESSMENT TABLE				
ASSET: COMMAND POST				
Attack Means	Criticality (C) (1 - 10)	Vulnerability (V) (1 - 10)	Threat Probability (TP) Y Value (1 - 10)	Risk Assessment (C x V x TP)
Small Arms Fire	9	1	9	81
Car/Truck Bomb	9	8	6	432
Chemical Weapon	9	8	1	72
Biological Weapon	9	8	1	72

Figure D-1. Example Asset Risk Assessment Table

is not filtered. A redundant command post exists; however, several hours would be required before it could be fully operational. Because the command post is necessary to carry out the mission, criticality is a 9 out of 10. The vulnerability is a 1 from small arms fire because small arms are unlikely to penetrate 12 inches of concrete and no windows exist to shoot into. The vulnerability from a car/truck bomb is higher because there is no traffic flow control around the building. The chemical warfare and biological warfare attack means are both high vulnerabilities because the ventilation system is unfiltered.

d. It is important to note that this rating system is not meant to be a precise science. It is one method of quantifying a subjective decision, in order to generally prioritize areas in terms of risk.

4. Risk Assessment

a. Figure D-1 gives the final RA for each asset. The assets can be prioritized based on the RA. The decision maker is required to determine the maximum amount of risk that is acceptable.

b. The risk can also be represented graphically using the RA graph, Figure D-2. The graph shall combine the Criticality/Vulnerability/Attack Means (the x-axis) and the Threat Probability (the y-axis) to represent the risk. The representative risk is an expression of the relative impact on an asset or a planning and response element, given a stated attack means. Representative risk does NOT attempt to forecast risk (e.g., assign predictability or likelihood).

c. No standard methodology exists for establishing risk levels and their determination shall vary from installation to installation, based on the commander's judgment. Although this process is subjective, commanders can focus their decision on where to establish the minimum risk by considering the following questions:

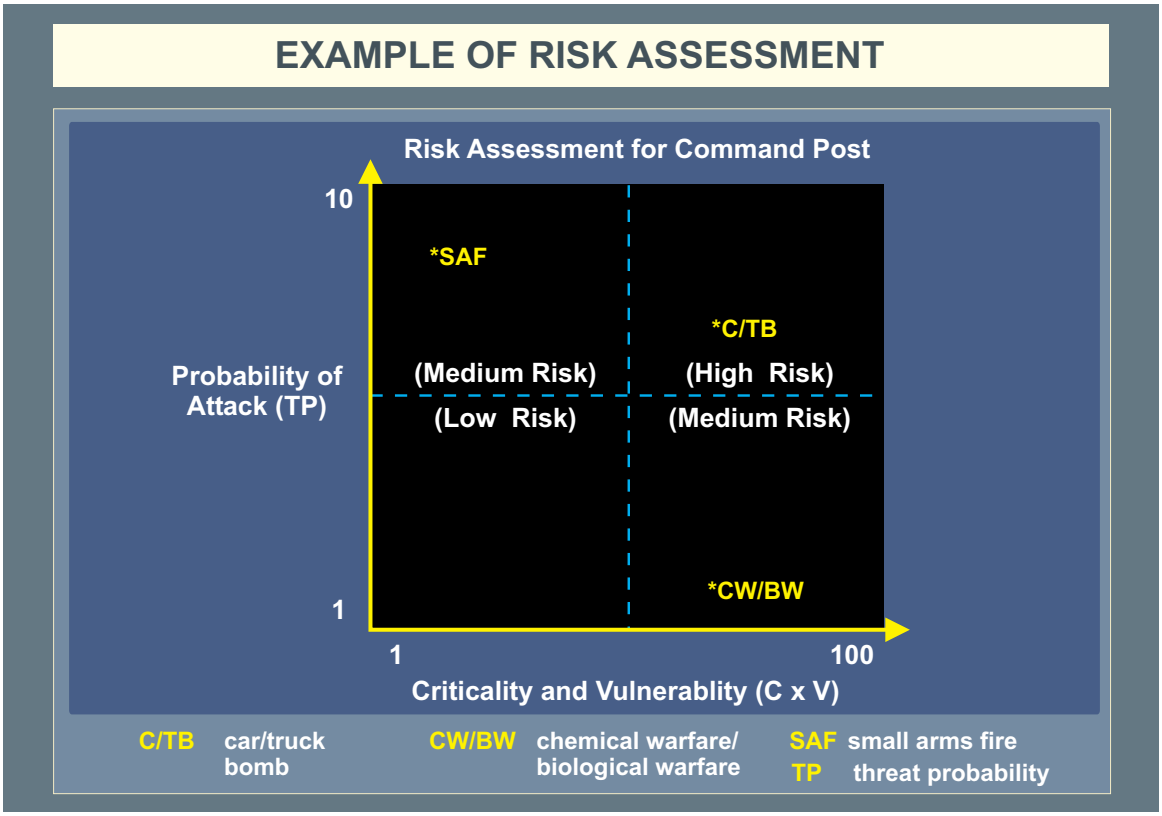


Figure D-2. Example of Risk Assessment

(1) What is the installation's mission? How important is that mission to overall US military objectives in the region? (Criticality Assessment)

(2) What resources are available for AT activities on the installation? (VA)

(3) Where are the nearest available resources that could augment the installation, should an incident occur? Does the commander have tasking authority for those resources? (VA)

5. Completing the Process — Risk Management

a. The end products of the above process shall be the identification of areas and assets that are vulnerable to the identified attack means and the development of associated assessment tables. From the information developed from all assessments (criticality, threat, vulnerability, and risk and the RA graph), the commander shall make a decision on how best to employ given resources and force protection measures to deter, mitigate, or prepare for a terrorist incident. Installation commanders should document their risk management methodology.

b. There are several ways to reduce risk. The decision maker does not easily control two of those methods, reducing the threat and reducing the criticality. The one method that is controllable is reducing the vulnerability of an asset.

c. Looking at the above example and considering only the command post, it is apparent that the highest risk is from a car/truck bomb. What are some ways of reducing the vulnerability?

(1) Set up barriers to control traffic flow around the command post. The further away a prospective car/truck bomb detonation, the less impact it will have on the intended target. Another alternative is to control the traffic coming onto the installation. If several buildings exist that require protection from car/truck bombs, then cars and trucks can be searched more thoroughly at the entrance to the facility. If bombs aren't allowed to enter the facility, then the risk is greatly reduced.

(2) Determine why it takes several hours to place the redundant command post in full operation. This may only require a simple policy change or pre-positioning of equipment but the result shall be less vulnerability due to redundancy.

d. At the end of the RA and risk management process, the commander must engage and concur with the entire assessment in order to focus the next steps in risk management process (taking action).

e. The use of CVAMP shall assist commanders and ATOs in this effort.

Intentionally Blank

APPENDIX E
SAMPLE ANTITERRORISM PLAN FORMAT

1. Overview

a. The format outlined below is offered as one means of developing an AT plan. It is optimized for a base or installation, but can be adapted for other facilities and deployed units. It is meant to help the AT officer structure the AT plan in a comprehensive and organized manner. The format is patterned after the standard five-paragraph military operation order (Situation-Mission-Execution-Administration and Logistics-Command and Signal).

b. This format enables the integration of existing programs such as law enforcement, physical security, AT, OPSEC, information security, high-risk personnel protection, and other installation efforts. AT plans should be integrated into all plans and separate annexes. Remember that staff interaction is a crucial element of developing a realistic, executable plan.

c. Although this sample is patterned after the military operation order, it applies to managers of DOD agencies and field activities as they develop plans to protect personnel, activities, and material under their control.

d. This sample uses supporting annexes, appendices, tabs, and enclosures to provide amplifying instructions as required. This method shortens the length of the basic plan (which should be read by all personnel outlined in the plan), and provides organization, structure, and scalability.

2. Sample Format

Installation/Operation Name
Location
Date/Time Group

INSTALLATION/OPERATION NAME ANTITERRORISM PLAN 2002 (AT-04)

Task Organization. (Include all agencies/personnel [base and civilian] responsible to implement the plan. Include as a separate Annex. See Annex A [Task Organization].)

Maps/Charts: (List all applicable maps or charts. Include enough data to ensure personnel are using the correct year/edition/version of the subject material.)

Time Zone: (Enter the time zone of the installation. Indicate the number of hours to calculate [plus/minus] ZULU time.)

Ref: (Enter the compilation of pertinent publications, references, MOU/MOA. This list may be included in a separate Annex. See Annex Q [References].)

1. SITUATION

a. General. This plan applies to all personnel assigned or attached to the installation. (Describe the political/military environment in sufficient detail for subordinate commanders, staffs, and units to understand their role in the installation AT operations.)

b. Enemy. (The enemy is any adversary capable of threatening the installation's personnel, facilities, and equipment. [The general threat of terrorism to this installation including the intentions and capabilities, identification, composition, disposition, location, and estimated strengths of hostile forces. Include the general threat of terrorist use of WMD against this installation. This information should remain unclassified when possible. See paragraph 1f, Intelligence, on identifying specific threats.] This information may be included as a separate Annex. See Annex B [Intelligence].)

c. Friendly. (The forces available [both military and civilian] to respond to a terrorist attack. Include the next higher headquarters and adjacent installations, and any units/organizations that are not under installation command, but may be required to respond to such an incident. These units/organizations may include HN and US military police forces, fire and emergency services, medical, and Federal/state and local agencies, special operations forces, engineers, detection [radiological, nuclear, biological, and chemical] decontamination or smoke units, and EOD. Include MOAs/MOUs and any other special arrangements that will improve forces available to support the plan. If in the US and its territories, the DOJ, FBI is responsible for coordinating all Federal agencies and DOD forces assisting in the resolution of a terrorist incident. If outside the US and its territories, the DOS is the lead agency. This information can be included in a separate Annex[s]. See Annex A [Task Organization] and Annex J [Command Relationships].)

d. Attachments/Detachments. (Installation/civilian agencies NOT normally assigned to the installation that are needed to support this plan. Explain interagency relationships and interoperability issues. This can be listed in other Annexes. See Annex A [Task Organization] and Annex J [Command Relationships].)

e. Assumptions. (List planning/execution assumptions.) All critical assumptions used as a basis for this plan. Assumptions are those factors unlikely to change during the implementation of the AT plan and that must be addressed in order to continue to plan. They can range from the installation's troop strength to addressing the local political/social environment. Examples follow:

(1) The installation is vulnerable to theft, pilferage, sabotage, and other threats. The installation is also vulnerable to a WMD attack.

(2) An act of terrorism involving WMD can produce major consequences that will overwhelm almost immediately the capabilities of the installation.

(3) Security personnel, both military and civilian, may be insufficient to provide total protection of all installation resources; therefore, the principal owner or user of a facility, resource, or personnel must develop adequate unit awareness and safeguard measures.

(4) No single unit on the installation possesses the expertise to act unilaterally in response to attacks.

(5) If protective equipment is not available, responders will not put their own lives at risk.

(6) Local, nonmilitary response forces will arrive within (time) of notification.

(7) Units specializing in WMD response will arrive on-site within (number of hours based on installation location) of notification.

(8) The HN is supportive of US policies, and will fulfill surge requirements needed to respond to a WMD incident in accordance with MOAs/MOUs.

f. Intelligence. (The person, staff, or unit responsible for intelligence collection and dissemination. The installation commander must have a system in place to access current intelligence. This can be included in Annex B [Intelligence].) (National-level agencies, combatant commanders, and intelligence systems provide theater or country threat levels and threat assessments. In the US and its territories, local installations must obtain the local terrorist threat information by querying the FBI through the installation's law enforcement liaison, local law enforcement, or other Federal agencies.) Obtain these assessments, as they will serve as a baseline for the installation's tailored assessment. The installation should have a process in place for developing the installation's tailored threat assessment or "local threat picture." The installation's tailored threat assessment should be continuously evaluated, updated, and disseminated, as appropriate, and as directed by the installation commander. The commander

should determine the frequency and the means of dissemination of the installation's tailored AT product. Note: Commanders cannot change the threat level, which is developed at the national-level although they can declare higher FPCONs than the baseline.

2. MISSION. (A clear, concise statement of the command's mission and the AT purpose or goal statement supporting the mission. The primary purpose of the AT plan is to safeguard personnel, property, and resources during normal operations. It is also designed to detect and deter a terrorist threat, enhance security and AT awareness, and to assign AT responsibilities for installation personnel.)

3. EXECUTION

a. Commander's Intent. (Commander's vision on how he/she sees the execution of the unit's AT program. Refer to Service planning doctrine for assistance.)

b. Concept of Operations. (How the overall AT operation should progress. This plan stresses deterrence of terrorist incidents through preventive and response measures common to all combatant commands and Services. During day-to-day operations, the installation should stress continuous AT planning and passive, defensive operations. This paragraph should provide subordinates sufficient guidance to act if contact or communications with the installation chain of command is lost or disrupted.)

(1) The installation's AT concept of operations should be phased in relation to pre-incident actions and post-incident actions. AT planning and execution requires that staff elements work with a much greater degree of cohesiveness and unity of mission than that required during the conduct of normal base sustainment operations. The AT mission, and the unpredictability of its execution, requires very specific "how to" implementation instructions of DOD FPCON measures and in what manner these actions must be coordinated. This "how to" element is not normally included in the concept of operations paragraph; however the necessity to provide "how to" guidance in the AT plan requires a different manner of data presentation to ensure brevity and clarity. The implementation instructions are put into the form of action sets and can be displayed in the form of an execution matrix (Pre-Incident Action Set Matrix).

(2) In post-incident planning, the installation should focus on its response and reconstitution responsibilities upon notification of a terrorist incident and the procedures for obtaining technical assistance/augmentation if the incident exceeds the installation's organic capabilities. National-level responders (Federal Emergency Management Agency [FEMA], Red Cross, and FBI) may not be immediately accessible or available to respond to an installation's needs. Therefore each installation must plan for the worst-case scenario, by planning its response based on its organic resources and available local support through MOA/MOUs.

(3) The situation may dictate that the installation not only conduct the initial response but also sustained response operations. Many installations do not have onboard WMD officers or response elements. This paragraph will include specific implementation instructions for all operational areas and the manner in which these actions must be coordinated. The implementation

instructions can be put in the form of actions sets and displayed in the form of a synchronization matrix (Post-Incident Action Set Synchronization Matrix). The synchronization matrix format clearly describes relationships between activities, units, supporting functions, and key events which must be carefully synchronized to minimize loss of life and to contain the effects of a terrorist incident.

c. Tasks. (The specific tasks for each subordinate unit or element listed in the Task Organization paragraph. Key members of the installation have responsibilities that are AT and/or WMD specific. The commander should ensure that a specific individual/unit/element within the installation is responsible for each action identified in this plan. Each individual/unit/element must know the tasks and responsibilities, what these responsibilities entail, and how these will be implemented. While the tasks and responsibilities for each AT planning and response element will be delineated in the pre- and post-incident action set matrices, it is recommended that the installation commander identify/designate the primary lead for each element and enter that information in this paragraph.)

(1) First Subordinate Unit/Element/Tenant

(a) Task Listing

d. Coordinating Instructions. This paragraph should include AT specific coordinating instructions and subparagraphs, as the commander deems appropriate. In addition, this section of the AT plan outlines aspects of the installation's AT posture that require particular attention to guarantee the most effective and efficient implementation of the AT plan. For the purposes of this plan, there are five basic coordinating instructions: 1) AT planning and response elements; 2) Procedural; 3) Security Posture; 4) Threat Specific Responsibilities; and 5) Special Installation Areas. The reader will be directed to specific Annexes that will provide amplifying instructions on these topics. The sections listed below are representative, and may not be all-inclusive.

(1) AT Planning and Response. For instructional purposes, this template outlines AT planning and response elements on the installation required to respond to a terrorist/WMD incident. Initial and sustained response to an attack must be a coordinated effort between the many AT planning and response elements of the installation, based on the installation's organic capabilities. As the situation exceeds the installation's capabilities, it must activate MOAs/MOUs with the local/state/Federal agencies (US and its territories) or HN (outside the US and its territories). For the purposes of this plan, an installation's capability is divided into AT planning and response elements.

AT Planning & Response Elements

Information & Planning *
Communications * +
HAZMAT *
Security * +
EOD +

Firefighting * +
Health & Medical Services * +
Resource Support *
Mass Care *
Public Works *
Intelligence Process +
Installation AT Plans/Programs +
Installation Perimeter Access +
Security System Technology +
Executive Protection +
Response & Recovery +
Mail Handling +

* Derived from FEMA emergency support functions
+ Derived from JSIVA assessment criteria

(2) Procedural

(a) Alert Notification Procedures. See Appendix 14 to Annex C (Operations).

(b) Use of Force/Rules of Engagement. See Annex H (Legal).

(c) Installation Training & Exercises. See Annex N (AT Program Review, Training & Exercises).

(d) Incident Response. See Appendix 1 to Annex C (Operations).

(e) Consequence Management. See Appendix 1 to Annex C (Operations).

(f) High-Risk Personnel Protection Procedures. See Appendix 9 to Annex C (Operations).

(g) AT Program Review. See Annex N (AT Program Review, Training & Exercises).

(h) Higher Headquarters Vulnerability Assessments. See Annex N (AT Program Review, Training & Exercises).

(3) Security Posture Responsibilities

(a) Law Enforcement. See Appendix 7 to Annex C (Operations).

(b) Physical Security to include Lighting, Barriers, Access Control. See Appendix 6 to Annex C (Operations).

(c) Other On-site Security Elements. See Appendix 8 to Annex C (Operations).

(d) Operations Security. See Appendix 10 to Annex C (Operations).

(e) Technology. See Appendix 15 to Annex C (Operations).

(f) EOC Operations. See Appendix 12 to Annex C (Operations).

(g) Critical Systems Continuity of Operations. See Appendix 13 to Annex C (Operations).

(h) Other.

(4) Threat Specific Responsibilities

(a) Antiterrorism. See Appendix 2 to Annex C (Operations).

(b) Weapons of Mass Destruction. See Appendix 5 to Annex C (Operations).

(c) Special Threat Situations. See Appendix 3 to Annex C (Operations).

(d) Information Security. See Appendix 11 to Annex C (Operations).

(e) Natural/Manmade Hazards (Optional). See Appendix 16 to Annex C (Operations).

(f) Other.

(5) Special Security Areas

(a) Airfield Security. See Appendix 4 to Annex C (Operations).

(b) Port Security. See Appendix 4 to Annex C (Operations).

(c) Embarkation/Arrival Areas. See Appendix 4 to Annex C (Operations).

(d) Buildings. See Appendix 4 to Annex C (Operations).

(e) Other.

4. ADMINISTRATION AND LOGISTICS. The administrative and logistic requirements to support the AT plan, which should include enough information to make clear the basic concept for planned logistic support. Ensure the staff conducts logistic planning for both pre- and post-incident measures addressing the following: locations of consolidated WMD defense equipment; expedient decontamination supplies; individual protective equipment exchange points; special

contamination control requirements; retrograde contamination monitoring sites; WMD equipment/supply controlled supply rates and pre-stockage points; and procedures for chemical defense equipment "push" packages. Specific logistic and administrative requirements will emerge throughout the planning process outlined in the concept of operations, specifically when developing the action sets. These requirements should be incorporated into this paragraph. Finally, include fiscal instructions on how to support AT operations.

a. Administration. See Annex O (Personnel Services).

b. Logistics. See Annexes D (Logistics) and E (Fiscal).

5. COMMAND AND SIGNAL. (Instructions for command and operation of communications-electronics equipment. Identify the primary and alternate locations of the command post and emergency operations center. Enter the installation's chain of command. Highlight any deviation from that chain of command that must occur as a result of a WMD incident. The chain of command may change based on the deployment of a JTF or a President or Secretary of Defense-directed mission. Identify the location of any technical support elements that could be called upon in the event of a terrorist incident and the means to contact each. Recommend the installation coordinate with higher headquarters to establish procedures to allow for parallel coordination to report a terrorist incident. The installation must provide for prompt dissemination of notifications and alarm signals, and the timely/orderly transmission and receipt of messages between elements involved in and responding to the incident.)

a. Command. See Annex A (Task Organization) and Annex J (Command Relationships).

b. Signal. See Annex K (Communications).

c. Command Post Locations

(1) Primary: (location)

(2) Alternate: (Location)

d. Succession of Command

(1) First alternate: (POSITION/TITLE)

(2) Second alternate: (POSITION/TITLE)

//SIGNATURE//
Commanding General/Officer
Signature Block

ANNEXES: (Should provide amplifying instructions on specific aspects of the plan. Each ANNEX can be subdivided into APPENDICES, TABS, and ENCLOSURES as required to provide amplifying instructions. Further, some of these supporting documents may be established in other unit operating orders/procedures, and referenced as required.)

ANNEX A – Task Organization (key AT organization composition e.g., AT Working Group, Crisis Management Team, Emergency Operations Center, First Response Elements).

Appendix 1 – DIA Threat Assessment or Service Worldwide Threat Assessment (e.g., United States Air Force installations, personnel, and resources)

Appendix 2 – Table of Organization

Appendix 3 – Post Prioritization Chart

ANNEX B – Intelligence (the agency[s] responsible for intelligence and specific instructions. In the US and its territories, commanders must obtain the local terrorist threat information by querying the FBI through the installation's law enforcement liaison, local law enforcement or other Federal agencies).

Appendix 1 – Local Threat Assessment

Appendix 2 – Local CBRNE Assessment, to include any TIM within or transiting the area of interest.

Appendix 3 – Local Criticality/Vulnerability Assessment

Appendix 4 – Risk Assessment

Appendix 5 – Pre-deployment AT Vulnerability Assessment

ANNEX C – Operations (this is the most IMPORTANT part of the plan). Annex C and supporting Appendices will provide specific instructions for all the various AT operations. All other Annexes/ Appendices support the implementation of Annex C.

Appendix 1 – Incident Planning and Response (how the various agencies [military/civilian] and resources will be integrated to respond to the operations outlined below. These instructions should be generic enough to apply across the range of operations. Specific instructions for each operation will be detailed in the appropriate Annex/Appendix/Enclosure).

Tab A – Incident Command and Control Procedures
Tab B – Incident Response Procedures
Tab C – Consequence Management Procedures

Appendix 2 – Antiterrorism

Tab A – Mission Essential Vulnerable Assets
Tab B – Potential Terrorist Targets
Tab C – FPCON
Enclosure 1 – FPCON Action Sets (Who/What/When/Where/How)
Tab D – Random Antiterrorism Measures Procedures

Appendix 3 – Special Threat Situations

Tab A – Bomb Threats
Enclosure 1 – Bomb Threat Mitigation
Enclosure 2 – Evacuation Procedures
Enclosure 3 – Search Procedures
Tab B – Hostage Barricaded Suspect
Tab C – Mail Handling Procedures

Appendix 4 – Special Security Areas

Tab A – Airfield Security
Tab B – Port Security
Tab C – Embarkation/Arrival Areas
Tab D – Buildings

Appendix 5 – Weapons of Mass Destruction (CBRNE) & HAZMAT (the specific procedures planning, training, and response to WMD [CBRNE] incidents. Care should be taken to integrate existing plans for response to HAZMAT incidents to avoid duplication. Include "baseline" preparedness.)

Tab A - WMD Action Set Synchronization Matrix (Who/What/Where/When/How)
Tab B – CBRNE Emergency Responder Procedures

Appendix 6 – Physical Security

Tab A – Installation Barrier Plan (procedures and pictorial representation of barrier plan.)
Tab B – Installation Curtailment Plan
Tab C – Construction Considerations
Tab D – Facility and Site Evaluation and/or Selection
Tab E – AT Guidance for Off-Installation Housing

Appendix 7 – Law Enforcement

Tab A – Organization, training, equipping of augmentation security personnel

Tab B – Alternate Dispatch Location
Tab C – Alternate Arming Point

Appendix 8 – Other On-Site Security Personnel

Appendix 9 – High-Risk Personnel

Tab A – List of High Risk Billets

Appendix 10 – Information Operations

Tab A – OPSEC
Tab B – Deception
Tab C – PSYOP
Tab D – Computer Network Operations
Tab E – Electronic Warfare

Appendix 11 – Information Security

Appendix 12 – Emergency Operations Center Operations (procedure for the activation and operations of the EOC)

Tab A – EOC Staffing (partial/full)
Tab B – EOC Layout
Tab C – EOC Messages and Message Flow
Tab D – EOC Briefing Procedures
Tab E – EOC Situation Boards
Tab F – EOC Security and Access Procedures

Appendix 13 – Critical Systems Continuity of Operations Plans (those systems that are essential to mission execution and infrastructure support of the installation, e.g., utilities systems, computer networks. This document outlines how the installation will continue to operate if one or more critical systems are disrupted or fail and how the systems will be restored.)

Tab A – List of installation critical systems
Tab B – Execution checklist for each critical system

Appendix 14 — Emergency Mass Notification Procedures (the specific means and procedures for conducting a mass notification. Also covered should be the procedures/means for contacting key personnel and agencies.)

Tab A – Situation Based Notification
Tab B – Matrix List of Phone Numbers/Email Accounts

Appendix 15 – Exploit Technology Advances (the process and procedures for developing and employing new technology. Identify who is responsible and what should be accomplished).

Appendix 16 – Higher Headquarters Vulnerability Assessments (procedures for conducting higher headquarters vulnerability assessments).

Appendix 17 – Natural/Manmade Hazards (optional) (hurricanes, flooding, chemical plants, etc.).

Tab A — Locality specific natural and manmade hazards

ANNEX D – Logistics (specific logistic instructions on how to support AT operations).

Appendix 1 – Priority of Work (the priority of employing scarce logistical resource)

Appendix 2 – Emergency Supply Services

Appendix 3 – Weapons and Ammunition Supply Services

Appendix 4 – Emergency Equipment Services

Appendix 5 – Evacuation Shelters

Appendix 6 – Generator Refueling Matrix

ANNEX E – Fiscal (specific fiscal instructions on how to support AT operations from pre-incident through post-incident).

Appendix 1 – AT Program Objective Memorandum Budget Submission Instruction

Appendix 2 – Combating Terrorism Readiness Initiatives Fund Submission Instructions

Appendix 3 – Fiscal Management During Exigent Operations

ANNEX F – Tenant Commanders (specific instructions on how tenant commands/agencies support AT operations).

Appendix 1 – Operational Areas (pictorial)

ANNEX G – Air Operations (specific air instructions on how to support AT operations).

Appendix 1 – List of Landing Zones (used for emergency medical evacuations or equipment/personnel staging areas)

Appendix 2 – Landing Zone Preparation Procedures

ANNEX H – Legal (the jurisdictional limits of the installation's commander and key staff. Although the DOJ, FBI, has primary law enforcement responsibility for terrorist incidents in the United States, the installation commander is responsible for maintaining law and order on the installation. For OCONUS incidents, the installation commander must notify the HN and the geographic combatant commander; the geographic combatant commander will notify DOS. Once a task force or other than installation support arrives on the installation, the agencies fall under the direct supervision of the local incident commander. In all cases, command of military elements remains within military channels. The installation should establish HN agreements to address the use of installation security personnel, other military forces, and HN resources that clearly delineate jurisdictional limits. The agreements will likely evolve into the installation having responsibility "inside the wire or installation perimeter" and the HN having responsibility "outside the wire or installation perimeter." There may be exceptions due to the wide dispersal of work and housing areas, utilities, and other installation support mechanisms that may require the installation to be responsible for certain areas outside of the installation perimeter).

Appendix 1 – Jurisdictional Issues

Appendix 2 – Use of Force and/or Rules of Engagement Instructions

Appendix 3 – Pictorial Representation of Installation Jurisdiction

ANNEX I – Public Affairs (specific PAO instructions on how to support AT operations).

Appendix 1 – Command Information Bureau Organization and Operation

Appendix 2 – Local/Regional Media Contact Information

ANNEX J – Command Relationships (Provides specific guidance on command relationships and military/civilian interoperability issues during incident command and control).

Appendix 1 – AT Organizational Charts (Crisis Management Team, AT Working Group, First Responder Elements, Incident Command Organization [include civilian and other external agencies].)

ANNEX K – Communications (specific communications instructions on how to support AT operations. Include systems/procedures for SECURE and NON-SECURE communications means.)

Appendix 1 – Installation AT Communication Architecture

Appendix 2 – Incident Command Communication Architecture

Appendix 3 – EOC Communication Architecture

Appendix 4 – Security Force Communication Architecture

Appendix 5 – Fire Department Communication Architecture

Appendix 6 – Medical Communication Architecture

Appendix 7 – Other Agencies

ANNEX L – Health Services (specific medical instructions on how to support AT operations).

Appendix 1 – Mass Casualty Plan

Appendix 2 – Procedures for Operating with Civilian Emergency Medical Service and Hospitals

ANNEX M – Safety (specific safety instructions on how to support AT operations).

ANNEX N – AT Program Review, Training, and Exercises

Appendix 1 – AT Program Review

Tab A – Local Assessments
Tab B – Higher Headquarters Assessments

Appendix 2 – AT Required Training

Appendix 3 – Exercises

ANNEX O – Personnel Services (administrative and personnel procedures required to support the plan, e.g., civilian overtime, posttraumatic stress syndrome counseling).

Appendix 1 – Operating Emergency Evacuation Shelters

ANNEX P – Reports (all the procedures for report submissions and report format).

Appendix 1 – Reporting Matrix

ANNEX Q – References (all supporting reference materials, publication, regulations etc.).

ANNEX R – Distribution (the list of agencies to receive this plan; overall plan classification, handling and declassification procedures).

APPENDIX F
ANTITERRORISM CHECKLIST

1. Introduction

Protection of DOD assets is an inherent obligation of military commanders. The following checklist is a self-assessment, management tool that can be used by the commander and/or antiterrorism officer to assess the status of his/her AT program. This checklist is structured around the AT Standards outlined in DODI 2000.16, *DOD Antiterrorism Standards*. Not all the standards are applicable to all levels of command, therefore, commanders and Service AT guidance should be used where applicable.

Checklist for Commanders/Managers to Evaluate Antiterrorism Program Adequacy

Program Review

_____ Is commander/antiterrorism officer (ATO) aware of and integrating other programs supporting FP?

_____ Do ALL installation units participate in random antiterrorism measures (RAMs)?

_____ Is the antiterrorism (AT) program comprehensive, current, and effective?

_____ Can the unit do the mission under force protection conditions (FPCONs) in use?

_____ Are critical FPCONs compromised for unit morale or convenience?

_____ ATO staff and resources sufficient, e.g., reliable and accessible SECRET Internet Protocol Router Network (SIPRNET) access?

_____ Is AT a routine element of daily mission planning and execution?

_____ Are operational patterns varied?

_____ Is operations security (OPSEC) included in mission planning?

_____ Does the unit continually monitor threat and corresponding security posture?

_____ Does the unit monitor and control access of visitors and employees in sensitive areas?

_____ Has the threat level changed since last vulnerability assessment (VA)?

_____ Is the threat assessment current and valid?

_____ Are RAMs having the desired effect on unit awareness, readiness, and deterrence?

_____ Does the unit have an AT program and security posture appropriate for mission and potential threat?

_____ AT officer appointed?

_____ Antiterrorism working group (ATWG) designated?

_____ Emergency Disaster Planning Officer with chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE) emergency response program management responsibilities designated?

_____ Defense Intelligence Agency (DIA), Service specific and/or Federal Bureau of Investigation (FBI) threat assessment current?

_____ VA current?

Checklist for Commanders/Managers to Evaluate Antiterrorism Program Adequacy (cont.)

_____ AT Level I training current?

_____ Have you reviewed Department of Defense Instruction (DODI) 2000.16, *DOD Antiterrorism Standards*, DODI 2000.18, *DOD Installation Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive Emergency Response Guidelines*, and appropriate commander/Service AT guidance?

_____ Is commander/Service AT guidance implemented?

Organize for AT

_____ Does unit have adequate focus on AT?

_____ Is unit ATO school trained?

_____ Are right functions represented in ATWG?

_____ Is ATWG active? Meeting minutes documented, open items follow-up and closed? Accomplishments?

Threat Assessment

Do threat assessments provided by DIA, Service counterintelligence, intelligence and/or FBI integrate with the local threat assessment process:

_____ Identify specific terrorist capabilities, weapons, and tactics (to include weapons of mass destruction [WMD])?

_____ Consider the vulnerability of the facilities and utilities?

_____ Consider the criticality of the facilities and utilities?

_____ Provide the necessary information to the commander to help tailor FPCONs?

_____ Have a review mechanism to provide up-to-date information?

_____ Is the unit aware of current and potential threats (conventional and WMD)?

_____ Have toxic industrial materials (TIMs), located in or transiting the area of interest, been identified and characterized for their potential threat?

_____ Do you know the DIA and/or FBI (continental US [CONUS]) assessed threat level for the area?

_____ Has the commander assigned higher local threat level?

_____ Is a formal intelligence assessment on hand and current?

_____ Relationship with supporting intelligence activity?

_____ Is counterintelligence or law enforcement support needed?

_____ Local information considered?

_____ Local information network established? Part of ATWG?

_____ Aggressive list of threat options identified?

_____ Program review within past 12 months?

Checklist for Commanders/Managers to Evaluate Antiterrorism Program Adequacy (cont.)

Vulnerability Assessment

_____ AT plan exercised within past 12 months?

_____ Has a local VA been conducted within the past year?

_____ Did the VA identify vulnerabilities and means to eliminate or mitigate them?

_____ Did the VA identify options for enhanced protection of Department of Defense (DOD) personnel and assets?

Does the AT VA assess the following functional areas at a minimum:

_____ AT plans and programs.

_____ Counterintelligence, law enforcement, liaison, and intelligence support.

_____ AT physical security measures.

_____ Vulnerability to a threat and terrorist incident response measures.

_____ VA for terrorist use of WMD/TIM.

_____ Availability of resources to support plans as written.

_____ Frequency and extent to which plans have been exercised.

_____ Level and adequacy of support from the host nation (HN), local community, and where appropriate, inter-Service and tenant organizations to enhance force protection (FP) measures or respond to a terrorist incident.

_____ Status of formal and informal agreements to support AT functions.

_____ Does the VA team contain expertise in order to meet the intent of providing comprehensive assessments?

_____ Is there a process to track and identify vulnerabilities through the chain of command?

Memorandum of Understanding / Memorandum of Agreement

_____ Is unit conforming to and employing memoranda of understanding (MOU) / memoranda of agreement (MOA) for local support?

_____ Does unit or any detached personnel fall under State Department for FP?

_____ Are State Department's FP instructions on hand for those individuals?

_____ Are organizations identified with jurisdiction for law enforcement, health, safety, and welfare of assigned Service members on and off duty?

_____ Is unit conforming to jurisdictional agreements in these areas (status of forces agreement [SOFA], interagency)?

_____ Are local community organizations with shared security interests (police, Federal law enforcement, hospitals, and public health) identified?

_____ Are mutual aid agreements in place with local community to leverage shared interests?

_____ Have mutual aid agreements been reviewed by higher headquarters (HQ)?

_____ Are mutual aid agreements executable (liability, jurisdiction, capabilities)?

Checklist for Commanders/Managers to Evaluate Antiterrorism Program Adequacy (cont.)

Mitigate Weapons of Mass Destruction Effects

_____ Has unit prepared for WMD attack?

_____ Does AT plan consider terrorist use of WMD (CBRNE)?

_____ Does the command have the procedures to process immediately through the chain of command reports of significant information obtained identifying organizations with WMD capability in their operational area?

_____ Is an estimate of terrorist potential use of WMD indicated in the local threat assessment?

_____ Procedures for detection of unconventional CBRNE attacks?

_____ Does unit training include awareness of indicators of unconventional attacks?

_____ Do all personnel have individual protective equipment available?

_____ Are collective protective systems available?

_____ Is CBRNE detection equipment available?

_____ Is decontamination equipment available?

_____ Are appropriate personnel familiar with procedure for obtaining CBRNE subject matter expertise assistance from DTRA or other source?

Antiterrorism Plan

_____ Is the AT plan signed?

_____ Does the installation incorporate AT planning into operation orders for temporary operations or exercises?

_____ Does the plan specify the AT mission and concept of operation?

_____ Does the plan layout the task organization and mission essential vulnerable areas?

_____ Does the plan include the risk management process, to include annual AT threat assessment with WMD coverage?

_____ Is there a process, based on local terrorism threat information, to raise FPCONs?

_____ Does the plan provide actions at each FPCON?

_____ Are site-specific AT measures linked to FPCONs classified, as a minimum, CONFIDENTIAL?

_____ Is the current FPCON measure adequate for the local threat?

_____ Does the plan provide a baseline for normal operations?

_____ Does plan provide diagram for RAMs?

_____ Does the plan include security force operations (including augmentation forces) and post priorities?

_____ Has the plan been reviewed within the past year to remediate procedural and resource shortfalls?

_____ Has the plan been approved by higher HQ?

Checklist for Commanders/Managers to Evaluate Antiterrorism Program Adequacy (cont.)

_____ Received/approved AT plans from lower HQ?

_____ Is the plan executable?

_____ Is the plan resourced?

_____ Does the plan mitigate vulnerabilities with policy and procedural solutions?

_____ Does the plan address response to incident and mass casualties?

Does the AT plan contain, as a minimum, site specific procedures for:

_____ Terrorism threat assessments?

_____ Vulnerability assessments?

_____ Program review?

_____ Training?

_____ AT physical security measures?

_____ Mass notification procedures?

_____ Incident response measures?

_____ Consequence management preplanned responses?

_____ AT considerations for plans/orders for temporary operations or exercises?

Does the command have an adequate "baseline" security posture to include:

_____ General AT and physical security awareness?

_____ Adequately equipped and trained first response forces?

_____ A security posture, capable of sustained operations and commensurate to the local threat, that adequately protects personnel and assets?

_____ Plans and procedures to transition from normal operations to an elevated state of readiness/execution?

_____ Is there a process for you to evaluate subordinate units' and/or tenant commands' knowledge and status of their AT responsibilities?

Training and Exercises

Are personnel receiving the appropriate levels of AT training to include:

_____ Level I training.

_____ Level II training.

_____ Level III training.

_____ Level IV training.

_____ Area of responsibility-specific training prior to deployment.

Checklist for Commanders/Managers to Evaluate Antiterrorism Program Adequacy (cont.)

_____ A system to track and document training.

_____ Is individual awareness of terrorism threat sufficient for threat environment/mission?

_____ Special local individual protective measures briefed and used?

_____ Has the command conducted field and staff training (annually) to exercise AT plans to include?

_____ AT physical security measures.

_____ Terrorist incident response measures.

_____ Terrorist consequence management preplanned responses.

_____ FPCON attainment procedures.

_____ Does the command maintain exercise after action reports/lessons learned and document actions taken to remediate identified shortfalls for at least a year?

Does command pre-deployment training include:

_____ Credible deterrence/response.

_____ Deterrence-specific tactics, techniques, and procedures.

_____ Terrorist scenarios and hostile intent decision making.

Antiterrorism Resources

_____ Does AT resource program support the required long-term security posture?

_____ Defined resource requirements to mitigate security deficiencies?

_____ Requirements justified with risk analysis?

_____ Alternative plans, policy, and procedural solutions considered or implemented?

_____ Does the command have a formal process to track, document, and justify resource requirements and identify resource shortfalls to higher HQ?

_____ Higher HQ approved these requirements?

_____ Does the command request Combatting Terrorism Readiness Initiative Find (CbT-RIF) for emergent and/or emergency commander AT requirements?

_____ Does the command incorporate AT requirements into the program objective memorandum (POM) submission?

_____ POM requirements submitted for out-year support of CbT-RIF funded investments?

_____ Status of CbT-RIF and POM requirements in the program/budget process?

_____ AT and security factors adequately weighed in acquisition and use of facilities (both temporary and permanent)?

_____ Current facilities conform to DOD and component AT military construction standards?

_____ Do structural engineers and security personnel work together to incorporate AT consideration in building design and review?

Checklist for Commanders/Managers to Evaluate Antiterrorism Program Adequacy (cont.)

_____ Are DOD AT standards for buildings incorporated into new constructions?

_____ Is technology being used to enhance security and human performance?

_____ Are technologies being identified as recommended/required for higher threat levels/FPCONs?

_____ Is the AT officer a member of the resource management committee?

Antiterrorism Officer Assigned in Writing

_____ Has the commander designated a Level II qualified/trained commissioned officer, noncommissioned officer, or civilian staff officer in writing as the ATO?

_____ For deploying organizations (e.g., battalion, squadron, ship) has at least one Level II qualified individual been designated in writing?

_____ Has the ATO attended a Service approved Level II AT training course?

Operations Security

_____ Have procedures been established that prevent terrorists from readily obtaining information about plans and operations (e.g., not publishing the commanding general's itinerary, safeguarding classified material, evaluating articles in installation publications)?

_____ Does the plan allow for in-depth coordination with the installation's OPSEC program?

_____ Has an OPSEC annex been included in the contingency plan?

Threat Information Collection and Analysis

_____ Has the commander tasked the appropriate organization under his/her command to gather, analyze, and disseminate terrorism threat information?

_____ Are personnel in the command encouraged and trained to report information on individuals, events, or situations that could pose a threat to the security of DOD personnel, families, facilities, and resources?

_____ Does the command have procedures to receive and process defense terrorism awareness messages and/or higher headquarters threat message?

_____ Does the command have technology to access critical terrorism intelligence (e.g., SIPRNET)?

Threat Information Flow

_____ Does the command forward all information pertaining to suspected terrorist threats, or acts of terrorism involving DOD personnel or assets for which they have AT responsibility up and down the chain of command?

_____ Does the command ensure there is intelligence sharing among all organizations?

_____ Does the command provide tailored threat information for transiting units?

Personnel Security

_____ Has the threat analysis identified individuals vulnerable to terrorist attack?

_____ Has a training program been established to educate both military and civilian personnel in the proper techniques of personnel protection and security commensurate with the local threat and the type of position held?

Checklist for Commanders/Managers to Evaluate Antiterrorism Program Adequacy (cont.)

Executive Protection and High-Risk Personnel Security

_____ Has the command identified high-risk billets and high-risk personnel to higher headquarters annually?

_____ Have personnel designated as "personnel at high-risk to terrorist attack" and "personnel assigned to high-risk billets" received appropriate AT training?

_____ Has the command annually reviewed and revalidated the protective services for executives?

_____ Has the command taken necessary measures to provide appropriate protective services for designated individuals in high-risk billets and high-risk personnel?

_____ Does the command review needs for supplemental security within 30 days of a change in the terrorism threat level?

Physical Security

_____ Does the installation commander coordinate and integrate subordinate unit physical security plans and measures into the AT plan?

_____ Are physical security measures considered, do they support, and are they referenced in the AT plan to ensure an integrated approach to terrorist threats?

Do AT physical security measures include provisions for the use of:

_____ Physical structures.

_____ Physical security equipment.

_____ Chemical, biological, radiological detection and protection equipment.

_____ Security procedures.

_____ RAMs.

_____ Response forces.

_____ Emergency measures sufficient to achieve the desired level of AT protection and preparedness to respond to terrorist attack.

_____ Are RAMs used for both in-place and transiting forces?

_____ Are special threat plans and physical security plans mutually supportive?

_____ Do security measures establish obstacles to terrorist activity (e.g., guards, HN forces, lighting, fencing)?

_____ Does the special threat plan include the threats identified in the threat statements of higher HQ?

_____ Does the physical security officer assist in the threat analysis and corrective action?

_____ Does the installation have and maintain detection systems and an appropriate assessment capability?

Checklist for Commanders/Managers to Evaluate Antiterrorism Program Adequacy (cont.)

Antiterrorism Guidance for Off-Installation Housing

_____ Are troops housed off-installation adequately secured?

_____ Do Service members in moderate, significant, and high threat areas receive instruction and supervision in residential security measures?

_____ In such areas, do unit AT response plans include current residence location information for all unit members residing off installation?

_____ In such areas, do units coordinate with local law enforcement authorities for protection of unit members residing off-installation (MOUs/MOAs/SOFAs)?

_____ Do incident response plans include measures for off-installation personnel (personnel warning system)?

_____ Does the command have procedures to ensure DOD personnel assigned to moderate, significant, and high terrorism threat level areas, who are not provided on-installation or other Government quarters, are furnished guidance on the selection of private residence to mitigate risk of terrorist attack?

_____ Does the command have procedures to conduct physical security reviews of off-installation residences for permanent- and temporary-duty DOD personnel in significant or high threat level areas?

_____ Based on these physical security reviews, does the command have procedures to provide AT recommendations to residents and facility owners?

_____ As suitable, does the command have procedures to recommend to appropriate authorities the construction or lease of housing on an installation or safer area?

_____ Does the command have procedures to complete residential security reviews prior to personnel entering into formal contract negotiations for the lease or purchase of off-installation housing in significant or high threat areas?

_____ Does the command have procedures to include coverage of private residential housing in AT plans where private residential housing must be used in moderate, significant, or high threat level areas?

In moderate, significant, or high threat areas, does the command incorporate family members and dependent vulnerabilities into antiterrorism assessment, mitigation, and reporting tools for:

_____ Facilities used by DOD employees and their dependents.

_____ Transportation services and routes used by DOD employees and their dependents.

_____ Has the SJA considered the ramifications of imposing these housing policies in CONUS and advised on the consequences?

Security Structure

_____ Does the AT plan indicate that the FBI has primary domestic investigative and operational responsibility in the United States and US territories?

_____ Has coordination with the SJA been established?

_____ Does the plan allow for close cooperation among principal agents of the military, civilian, and HN communities and Federal agencies?

Checklist for Commanders/Managers to Evaluate Antiterrorism Program Adequacy (cont.)

_____ Does the plan clearly indicate parameters for use of force, including the briefing of any elements augmenting military police assets?

_____ Is there a mutual understanding among all local agencies (e.g., military, local FBI resident or senior agent-in-charge, HN forces, and local law enforcement) that might be involved in a terrorist incident on the installation regarding authority, jurisdiction, and possible interaction?

_____ Has the staff judge advocate considered ramifications of closing the post (e.g., possible civilian union problems)?

_____ Does the AT plan identify the Department of State as having primary investigative and operational responsibility overseas?

Operations Center

_____ Has the operational command and coordination center (operations center) been established and exercised?

_____ Is the operational command and coordination center based on the needs of the installation while recognizing manpower limitations, resource availability, equipment, and command?

_____ Does the plan include a location for the operations center?

_____ Does the plan designate alternate locations for the operations center?

_____ Does the plan allow for the use of visual aids (chalkboards, maps with overlays, bulletin boards) to provide situation status reports and countermeasures?

_____ Does the plan create and designate a location for a media center?

_____ Have the operations and media centers been activated together within the last quarter?

_____ Does the operations center have standing operating procedures covering communications and reports to higher HQ?

_____ Does the operations center offer protection from terrorist attack?

Terrorist Incident Response Measures (first response)

Has the command prepared installation-wide and/or shipboard terrorist incident response measures which include:

_____ Procedures for determining the nature and scope of the terrorist incident and required response.

_____ Procedures for coordinating security, fire, and medical first responders.

_____ Steps to reconstitute the installation's ability to perform AT measures

_____ In moderate, significant, or high terrorist threat level areas, has the command included residential location information for all DOD personnel and their dependents in their incident response measures?

Checklist for Commanders/Managers to Evaluate Antiterrorism Program Adequacy (cont.)

Rules of Engagement / Rules for the Use of Force

_____ Does unit have correct rules of engagement (ROE) / rules for the use of force (RUF) guidance for the mission and environment?

_____ Do plan/current procedures provide enough "stand-off" to determine hostile intent and make proper decision to use force?

_____ Are troops trained for making ROE/RUF decisions in realistic situations?

_____ Are ROE/threat scenarios adequate and rigorous?

_____ Is unit prepared to apply ROE/RUF for threat scenarios?

Terrorist Consequence Management Preplanned Responses

_____ Do consequence management (CM) preplanned responses provide for appropriate emergency response and disaster planning and/or preparedness to respond to a terrorist attack for the installation and/or base engineering, logistics, medical, mass casualty response, transportation, personnel administration, and local and/or HN support?

_____ Do CM preplanned responses include guidelines for pre-deployment and garrison operations, pre-attack procedures, actions during attack, and postattack actions?

Community Engagement

_____ Has community engagement been considered in AT planning and operations?

_____ Has training considered community engagement?

_____ Do local intelligence personnel have access to community engagement information?

General Observations

_____ Was the AT plan developed as a coordinated staff effort?

_____ Does the AT plan outline reporting requirements (e.g., logs, journals, after-action report)?

_____ Does the AT plan address presence of the media?

_____ Does the AT plan include communications procedures and communications nets?

_____ Does the AT plan consider the possible need for interpreters?

_____ Does the AT plan consider the need for a list of personnel with various backgrounds to provide cultural profiles on foreign subjects and victims, as well as to assist with any negotiation efforts?

_____ Does the AT plan provide for and identify units that will augment military police assets?

_____ Does the AT plan delineate specific tasking(s) for each member of the operations center?

_____ Does the AT plan provide for a response for each phase of antiterrorism activity (e.g., initial response, negotiation, assault)?

_____ Does the AT plan designate Service support communications?

Checklist for Commanders/Managers to Evaluate Antiterrorism Program Adequacy (cont.)

_____ Does the AT plan make provisions for notification of accident and incident control officer?

_____ Does the AT plan provide for explosive ordinance disposal support?

____ Does the AT plan take into consideration the movement from various locations, including commercial airports, of civilian and military advisory personnel with military transportation assets?

_____ Does the AT plan allow for the purchase and/or use of civilian vehicles, supplies, food, if needed (including use to satisfy a hostage demand)? Does the AT plan make provisions for paying civilian employees overtime if they are involved in a special threat situation?

_____ Does the AT plan take into consideration the messing, billeting, and transportation of civilian personnel?

_____ Do appropriate personnel have necessary language training?

_____ Is military working dog support available?

_____ Does the command review its own and subordinate AT programs and plans at least annually to facilitate AT program enhancement?

_____ Does the command review the AT plan when the terrorist threat level changes?

_____ Has the command developed a prioritized list of AT factors for site selection for facilities, either currently occupied or under consideration for occupancy by DOD personnel? AT factors should include, but not limited to, screening from direct fire weapons, building separation, perimeter standoff, window treatments, protection of entrances and exits, parking lots and roadways, standoff zone delineation, security lighting, external storage areas, mechanical and utility systems.

_____ Has the command used these factors to determine if facilities can adequately protect occupants against terrorism attack?

APPENDIX G
SAMPLE BARRIER PLAN

1. Introduction

The following is a sample extract from a barrier plan for base X-Ray. The purpose of the diagrams is to show the information needed in basic barrier planning. Without background threat, vulnerability, criticality, and mission information, it is difficult to determine specifically why certain areas of this fictitious base are protected at different times or why they do not need more barriers at different FPCONs. Barrier plan considerations and research requirements listed in Chapter VI, "Preventive Measures and Considerations," have been considered elsewhere. The complete barrier plan would have tabs for each FPCON, which provide more detail and specify exact barrier locations.

2. Example

a. In this example, the first page (Figure G-1) gives an overview of the base with all areas identified. The various areas, buildings, and facilities have been identified and each has individual requirements based on the FPCON. The overview slide also provides a point of contact and outlines basic resource requirements to accomplish the effort.

b. The second page (Figure G-2) is a tab to the overall plan and shows detail for protecting "Area S." The premise in this sample plan reveals that the installation commander only plans to enclave this area during FPCONs C/D.

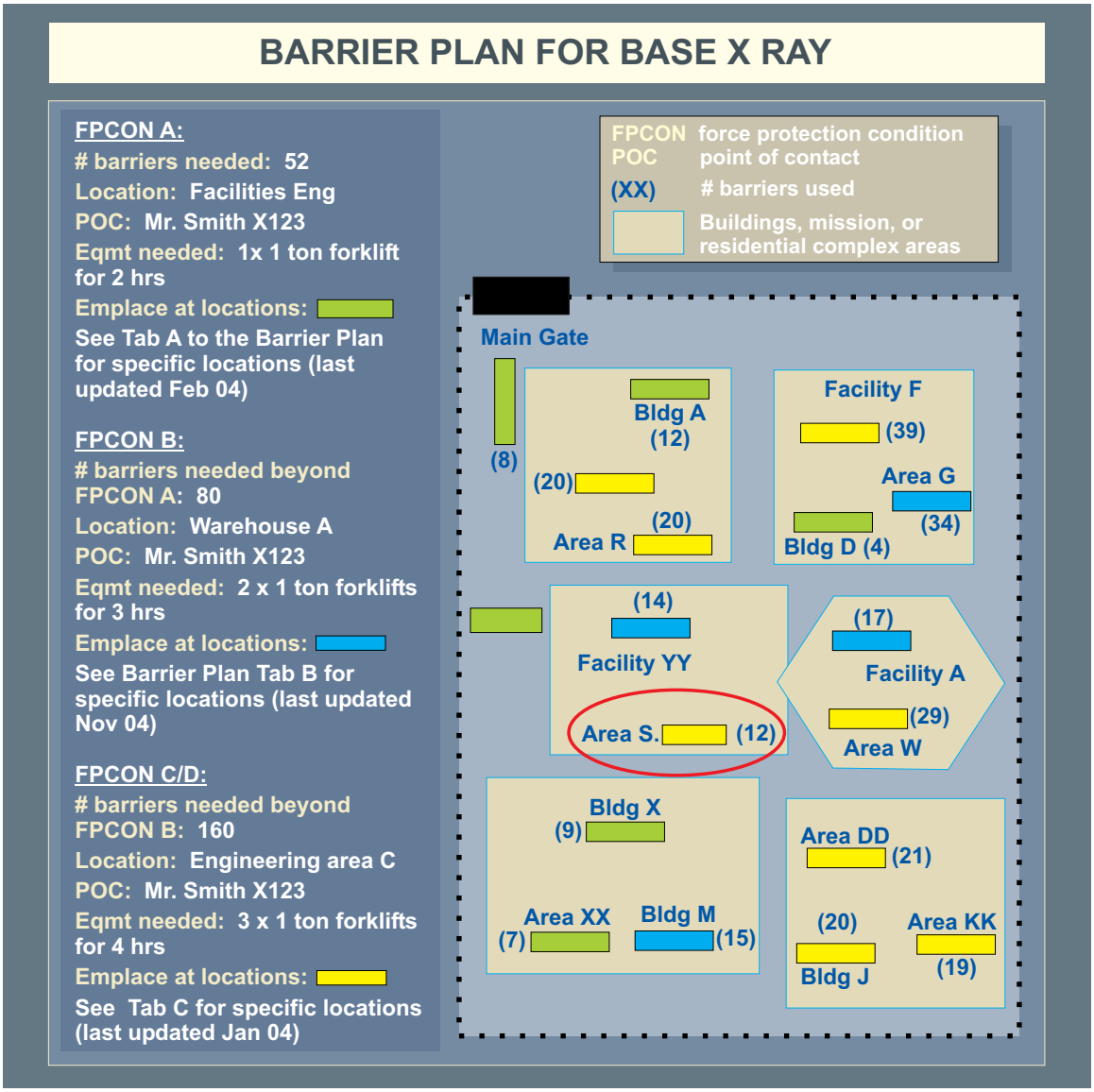


Figure G-1. Barrier Plan for Base X-Ray

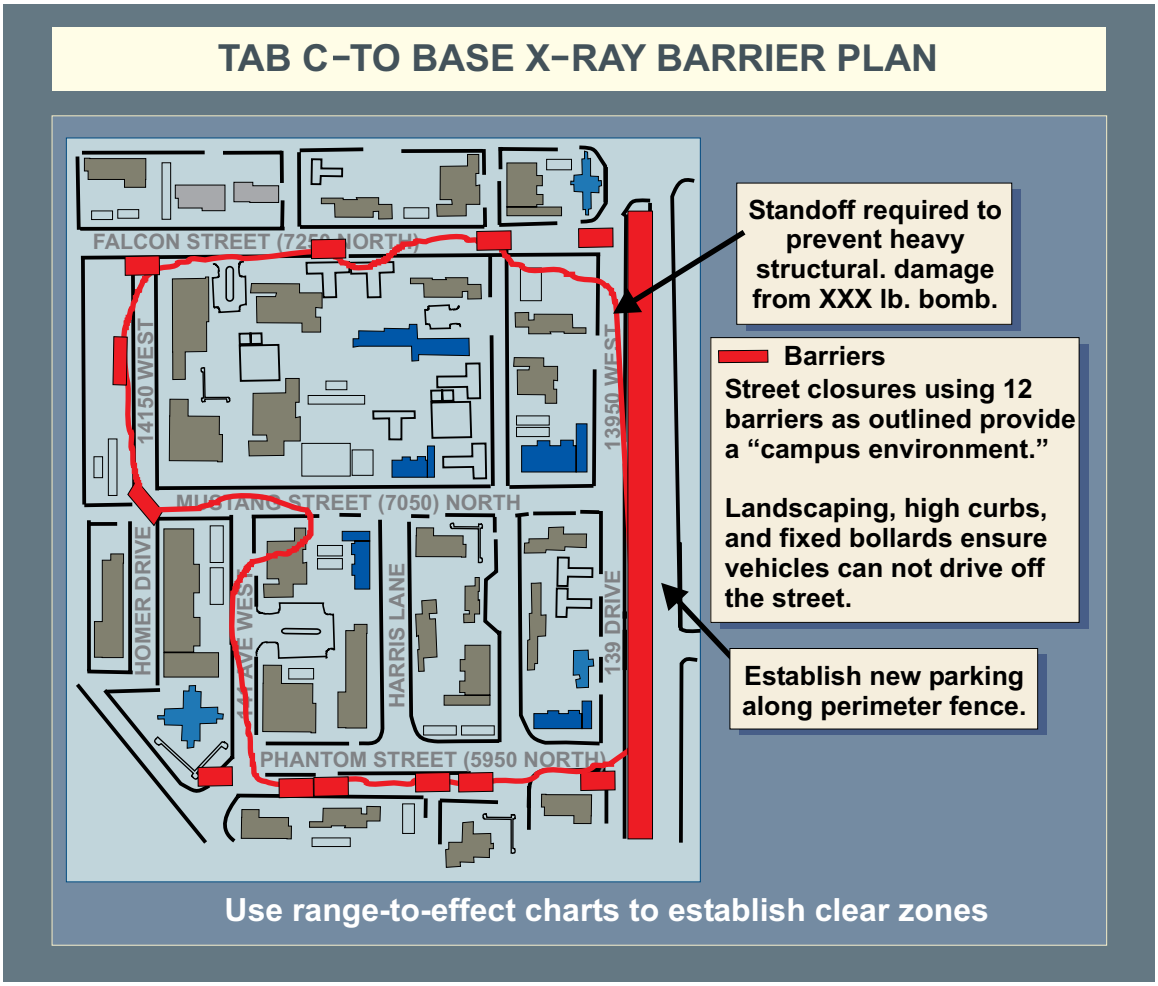


Figure G-2. Tab C- to Base X-Ray Barrier Plan

Intentionally Blank

APPENDIX H
FORCE PROTECTION CONDITION SYSTEM

1. General

a. FPCONs describe the progressive level of countermeasures in response to a terrorist threat to US military facilities and personnel as directed by DODD 2000.12, *DOD Antiterrorism (AT) Program*. These security measures are approved by the Joint Chiefs of Staff and are designed to facilitate inter-Service coordination and support of US military AT activities. They are outlined in DOD O-2000.12-H, DODI O-2000.16, *DOD Antiterrorism Handbook*, Appendix 3, *DOD FPCON System*. When installations adapt these measures for their site-specific circumstances, they should account for, as a minimum, combatant commander/Service requirements, local laws, and SOFAs. Per DODI 2000.16, *DOD Antiterrorism Standards*, FPCON measures are FOR OFFICIAL USE ONLY. An AT plan with a complete listing of site-specific AT measures, linked to an FPCON, shall be classified, as a minimum, CONFIDENTIAL. When separated from the AT plan, specific measures and FPCON measures remain FOR OFFICIAL USE ONLY.

b. The FPCON system is the principal means through which a military commander or DOD civilian exercising equivalent authority applies an operational decision on how to best guard against the threat. These guidelines shall assist commanders in reducing the effect of terrorist and other security threats to DOD units and activities.

c. Creating additional duties and/or watches and heightening security enhance the command's personnel awareness and alert posture. These measures display the command's resolve to prepare for and counter the terrorist threat. These actions shall convey to anyone observing the command's activities that it is prepared and an undesirable target, and that the terrorist(s) should look elsewhere for a vulnerable target.

d. The DOD system is generally not applicable to DOD elements for which the COM has security responsibility, and may have limited application to DOD elements that are tenants on installations and facilities not controlled by US military commanders or DOD civilian exercising equivalent authority. Still, commanders of US elements on non-US installations can execute many FPCON measures that do not involve installation level actions, at least to a limited degree. The terminology, definitions, and specific recommended security measures are designed to facilitate inter-Service coordination and support for the CbT efforts of the DOD components.

2. Force Protection Conditions

There are five FPCONs. Supporting measures for each condition are listed in Appendix 3 of DOD O-2000.12-H. The circumstances that apply and the purposes of each protective posture are as follows:

a. FPCON NORMAL applies when a general global threat of possible terrorist activity exists and warrants a routine security posture.

b. FPCON ALPHA applies when there is an increased general threat of possible terrorist activity against personnel or facilities, the nature and extent are unpredictable. ALPHA measures must be capable of being maintained indefinitely.

c. FPCON BRAVO applies when an increased or more predictable threat of terrorist activity exists. Sustaining BRAVO measures for a prolonged period may affect operational capability and relations with local authorities.

d. FPCON CHARLIE applies when an incident occurs or intelligence is received indicating some form of terrorist action or targeting against personnel or facilities is likely. Prolonged implementation of CHARLIE measures may create hardship and affect the activities of the unit and its personnel.

e. FPCON DELTA 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 imminent. Normally, this FPCON is declared as a localized condition. FPCON DELTA measures are not intended to be sustained for substantial periods.

3. Force Protection Condition Responsibilities

a. Geographic combatant commanders shall ensure that FPCONs are uniformly implemented and disseminated within their AOR.

(1) All military commanders and DOD civilians exercising equivalent authority are responsible for ensuring that their subordinates fully understand FPCON declaration procedures and FPCON measures.

(2) While there is no direct correlation between threat reporting and FPCONs, such information assists commanders in making prudent FPCON declarations. Existence of threat reporting in and of itself should not be the only factor used in determining FPCONs. FPCON declaration should be based on multiple factors that may include, but are not limited to, threat, target vulnerability, criticality of assets, security resource availability, operational and physiological impact, damage control, recovery procedures, international relations, and planned US Government actions that could trigger a terrorist response.

b. The FPCON system allows all military commanders and DOD civilians exercising equivalent authority the flexibility and adaptability to develop and implement AT measures that are more stringent than those mandated by higher authorities whenever FPCONs are invoked. Each set of FPCON measures is the minimum that must be implemented when a change in local threat warrants a change in FPCON or when higher authority directs an increase in FPCON. Authorities directing implementation may augment their FPCON by adding measures from higher FPCONs as necessary.

(1) Military commanders or DOD civilians exercising equivalent authority may implement additional FPCON measures from higher FPCONs on their own authority, develop

additional measures specifically tailored for site-specific security concerns, or declare a higher FPCON for their operational area/installation.

(2) Subordinate military commanders or DOD civilians exercising equivalent authority at any level may not lower an FPCON or implement measures that are less rigorous than those appropriate for the declared FPCON. Waivers for not complying with prescribed FPCON measures may be obtained by following the procedures in paragraph 6 below.

(3) It is essential for military commanders and DOD civilians exercising equivalent authority to implement formal analytical processes that result in a set of operational area or locality-specific terrorist threat indicators and warnings for use when transitioning from lower to higher FPCONs. Threat credibility, and if known, duration, operational environment (both HN and DOD), asset criticality, mission impact and measures in place that contribute to mitigating the current threat are but a few of the important elements commanders should consider when calibrating FPCON postures. Such processes and measures should be harmonized to the maximum degree possible, taking fully into account differences in threat, vulnerability, criticality, and risk of resources requiring protection.

(4) Military commanders, DOD civilians exercising equivalent authority, and their staffs shall examine the threat, physical security, terrorist attack consequences, and mission vulnerabilities in the context of specific DOD activities and the declared FPCON. When factors are combined and the collective terrorist threat exceeds the ability of the current physical security system (barriers, surveillance and detection systems, security personnel, and dedicated response forces) to provide the level of asset protection required, then implementation of higher FPCONs or additional measures is appropriate.

4. Force Protection Condition Management and Implementation

Implementation of FPCONs does not come without adverse effects on day-to-day operations; the additional costs can be measured and described both quantitatively and qualitatively. The DOD FPCON system acknowledges cost as a significant factor bearing on the selection and maintenance of FPCONs. FPCONs ALPHA and BRAVO include measures that can be sustained for extended periods, consistent with the terrorist threat.

5. Random Antiterrorism Measures Management and Implementation

a. Commanders and DOD civilians exercising equivalent authority should randomly change their AT TTP so that they ensure a robust security posture from which terrorists cannot easily discern patterns or routines that are vulnerable to attack. An effective RAM program shall enable security to appear not only formidable but also unpredictable and ambiguous to instill uncertainty in terrorist planning. The basic approach for RAMs program is to select security measures from higher FPCONs, as well as other measures not normally associated with FPCONs (command developed measures, or locally developed site-specific measures) that can be employed in a random manner to supplement the basic FPCON measures already in place. Using a variety of additional security measures in a normal security posture prevents overuse of security personnel,

as would be the case if a higher FPCON were to be maintained for an extended period of time. Selected RAMs offer an alternative to full implementation of a higher FPCON level. This is particularly important when terrorist threat estimates suggest that lower FPCONs may not, for the moment, be adequate in view of the risk, vulnerability, and criticality of DOD assets at the installation or facility.

b. To enhance the overall effectiveness of a given FPCON, unit commanders shall develop and implement a RAMs program as an integral part of their AT program. RAMs should be implemented in a strictly random manner, never using a set time frame or location for a given measure. RAMs should be visible (to confuse surveillance attempts) and should involve the command as a whole, not just the security personnel. To be effective, tenant and transient units must be fully integrated into and support the installation or facility RAM program. Advantages of implementing RAMs include, but are not limited to:

(1) Enables commanders/directors to maintain/sustain a lower FPCON without compromising security effectiveness. Also, it maximizes scarce security resources and minimizes security force burnout and degradation in command AT awareness.

(2) Makes it more difficult, through variations in security routines, for terrorists to target important assets, build detailed descriptions of significant routines, or predict activities by a specific asset or within a targeted facility or installation. An installation's tactical deception plan can be bolstered by the use of RAMs.

(3) Helps mask our capabilities to respond to, and defeat, terrorist attacks through unannounced, unpredictable, and visible security measures.

(4) Increases AT awareness for DOD personnel, their family members, visitors, and neighbors.

(5) Provides additional training and increases alertness of assigned security personnel and other participants through mental stimulation by changing their routine.

(6) Validates the installation or facility's capability to execute individual measures from higher FPCON.

(7) Provides a means to test the procedure, utilizing various methods, resources, and personnel to ensure it can be effectively implemented in an emergency.

(8) Enables commanders/directors to more rapidly transition between FPCONs.

c. In summary, commanders/DOD civilians exercising equivalent authority and their AT officers should keep the following tenets in mind when developing and executing their RAM program.

(1) The installation ATO is in charge of the RAM program, not the provost marshal or security officer if a separate entity/individual. However, the ATO should coordinate with the provost marshal/security officer regarding RAMs that require utilization of security personnel. The ATO should monitor, track, and analyze RAM implementation efforts.

(2) A RAM program is part of a proactive and dynamic AT program.

(3) RAMs should include visible actions in order to confuse surveillance attempts and should involve the command as a whole, not just the security personnel.

(4) To be effective, tenant and transient units must be fully integrated into and support the installation or facility RAM program.

(5) RAMs should be used throughout all FPCON levels and should include other measures not normally associated with an FPCON level such as command developed measures, or locally developed site-specific measures.

(6) To confuse terrorist surveillance attempts, RAMs should be implemented in a strictly irregular fashion, never using a set time frame or location for a given measure.

(7) Local RAMs should:

(a) Assess local threat capabilities and identify effective RAMs countermeasures.

(b) Mitigate installation/facility vulnerabilities.

(c) Be conducted both internally to the installation and externally in coordination with local authorities.

(d) Be compatible/coordinated with ongoing approved surveillance detection and security measures.

(e) Not be limited to security force personnel.

(f) Incorporate analysis of time and space considerations to allow security personnel to maintain sufficient standoff while determining hostile intent.

d. A dynamic and proactive RAM program visibly communicates a command's resolve to prepare for and counter the terrorist threat. A RAM program shall make it difficult for terrorist planners to discern security and defense and operational patterns. The terrorists should be compelled to look elsewhere for a more static, and therefore, more vulnerable target.

6. Deviations From Directed Force Protection Conditions

If it is determined that certain FPCON measures are inappropriate for current operations, or for proper threat mitigation, military commanders or DOD civilians exercising equivalent authority may request a waiver. The first general/flag officer exercising TACON for FP or DOD civilian member of the senior executive service (SES) exercising equivalent authority in the chain of command is the approval authority for waiver of specific FPCON measures. Geographic combatant commanders, their deputies, or DOD civilians exercising equivalent authority, may delegate this authority below the general/flag officer level on a case-by-case basis. Any senior military commander having TACON for FP or DOD civilian member of the SES exercising equivalent authority may withdraw first general/flag officer or DOD civilian authority and retain this authority, at his or her discretion. Waiver authority for specific FPCON measures directed by a higher echelon (above first general/flag officer or DOD civilian member of the SES) rests with the military commander or DOD civilian exercising equivalent authority directing their execution. Nothing in this waiver process is intended to diminish the authority or responsibility of military commanders or DOD civilians exercising equivalent authority, senior to the waiver authority, to exercise oversight of FPCON and RAMs program execution.

a. To ensure a consistent FP posture is maintained, tenants on US installations and facilities shall coordinate waiver actions with the host installation before submitting them to their chain of command.

b. All waiver requests shall be directed to the waiver authority. Information copies shall be sent to the combatant command's joint operations center, major/fleet command's operations center, service operations center, or DOD civilian operations center, as applicable.

c. Approved waivers, to include mitigating measures or actions, must be forwarded to Service, combatant command, major command, fleet, or DOD civilian equivalent command-level recipients within 24 hours.

7. Basic Force Protection Condition Procedures

a. Once an FPCON is declared, all listed security measures are implemented immediately unless waived by competent authority as described above. The declared FPCON should also be supplemented by a system of RAMs in order to complicate a terrorist group's operational planning and targeting. Specific measures for each FPCON are listed in DOD O-2000.12-H, Appendix 3.

(1) Airfield specific measures are for installations and facilities with a permanently functioning airfield. Installations and facilities with an emergency helicopter pad should review and implement any applicable airfield specific measures when they anticipate air operations.

(2) Due to their specific security requirements, DOD ships' measures are listed separately. Those measures applying solely to US Navy combatant ships are further identified. Shipboard guidelines are specially tailored to assist commanding officers and ship masters in reducing the effect of terrorist and other security threats to DOD combatant and noncombatant

vessels, to include US Army and Military Sealift Command ships worldwide. They provide direction to maximize security for the ship based on current threat conditions consistent with performance of assigned missions and routine functions.

b. Several factors influence specific countermeasures:

(1) Ability to maintain highest state of operational readiness.

(2) Measures to improve physical security through the use of duty and guard force personnel limit access to the exposed perimeter areas and interior of the unit/facility by hostile persons, and barriers to physically protect the unit/facility.

(3) Availability of effective command, control, and communication systems with emphasis on supporting duty/watch officers, security personnel, and key personnel.

(4) An AT awareness program for all personnel.

(5) Protection of high-risk assets and personnel.

(6) Measures necessary to limit activities, and visitor/social engagements.

c. FPCON NORMAL and all FPCON levels should include site specific measures a facility commander deems necessary when establishing a baseline posture.

Intentionally Blank

JURISDICTIONAL AUTHORITY FOR HANDLING TERRORIST INCIDENTS					
LOCATION	INITIAL RESPONSE	PRIMARY AUTHORITY/ JURISDICTION	PRIMARY ENFORCEMENT RESPONSIBILITY	EXERCISING CONTROL OF MILITARY ASSETS	PRIMARY INVESTIGATIVE RESPONSIBILITY
WITHIN THE UNITED STATES					
ON BASE	MILITARY POLICE	FBI/INSTALLATION COMMANDER	FBI/INSTALLATION COMMANDER	INSTALLATION OR UNIT COMMANDER (SUPPORT FBI)	FBI/NCIS/PMO CID/AFOSI
OFF BASE	CIVIL POLICE	FBI/CIVIL POLICE	FBI/CIVIL POLICE		FBI
OUTSIDE THE UNITED STATES					
ON BASE	MILITARY POLICE	HOST GOVERNMENT/DOS INSTALLATION COMMANDER	HOST GOVERNMENT/DOS INSTALLATION COMMANDER	INSTALLATION OR UNIT COMMANDER (IAW APPLICABLE STATUS-OF-FORCES AGREEMENT OR OTHER BILATERAL AGREEMENTS GOVERNING THE EMPLOYMENT OF MILITARY FORCES)	HOST GOVERNMENT/ NCIS/PMO CID AFOSI
OFF BASE	HOST-COUNTRY LAW ENFORCEMENT	HOST GOVERNMENT/DOS	HOST GOVERNMENT/DOS	INSTALLATION OR UNIT COMMANDER (IAW APPLICABLE STATUS-OF-FORCES AGREEMENT OR OTHER BILATERAL AGREEMENTS GOVERNING THE EMPLOYMENT OF MILITARY FORCES)	HOST GOVERNMENT WITH SUPPORT FROM US LAW ENFORCEMENT AGENCIES AS PROVIDED FOR IN BILATERAL AGREEMENTS
NOTE:	Coordinate with the local staff judge advocate to clarify authority and questions of jurisdiction. Coordinate with Department of State officials as required. Coordinate in advance with local law enforcement agencies to ensure that support procedures are in place and established information/communication channels are functioning.				

Figure J-1. Jurisdictional Authority for Handling Terrorist Incidents

JURISDICTIONAL AUTHORITY FOR HANDLING TERRORIST INCIDENTS (cont'd)	
AFOSI	Air Force Office of Special Investigations
CID	Criminal Investigation Division
DOS	Department of State
FBI	Federal Bureau of Investigation
IAW	in accordance with
NCIS	Naval Criminal Investigative Service
PMO	provost marshal's office

Figure J-1. Jurisdictional Authority for Handling Terrorist Incidents (cont'd)

APPENDIX K
THREAT INFORMATION ORGANIZATION MATRIX

1. Introduction

The following matrix (see Figure L-1) is provided as a tool that could be used to categorize, organize, and analyze threat information relevant to an antiterrorism program. It is similar to an intelligence collection plan, but is intended for use on installations. If an intelligence collection plan is already active on the installation or base, the ATO should endeavor to have AT efforts integrated with ongoing efforts.

2. Organization Matrix

a. The basic premise of this organization matrix is that there are several key questions (PIRs) that the command needs to answer in order to keep the installation better protected or aware of potentially developing terrorist activity. These PIRs have supporting components or related questions (IRs). Individual indicators suggest when the IR is active. The indicators are then divided into their core elements (specific information requirements [SIRs]) that installation staff members or coordination agencies need to report or record. Similarly, for a given incident, such as a stolen identification card, that information can be traced back to a bigger question and suggest that someone is conducting surveillance on the base or nearby base.

b. The SIRs should be given to the staff members who would likely observe or see the types of information suggested. For instance, gate guards should be given the SIRs to report unauthorized access attempts (item 1.32a) (Column D row 28), but the installation information technology office would be responsible for reporting computer viruses, unauthorized attempts to access the network, etc. (items 1.16a, 1.16b). The organization plan also assists the ATO in explaining to coordinating agencies exactly what information is expected.

c. There is no requirement to use this or other threat information organization models, but if used, should be modified to fit specific commander and installation requirements, agreements, and efforts.

d. Within the US, intelligence oversight regulations remain in effect. AT officers and analysts should not endeavor to collect or maintain information on individuals, but may track AT related events and activities. AT officers should coordinate their threat organization activities with law enforcement or intelligence officials.

INSTALLATION THREAT INFORMATION ORGANIZATION PLAN

				Collection		Collection Agencies																
PIR	**IR**	**Indicators**	**Specific Information Requirements (SIRs)**	**Date Info needed**	**Date info no longer needed**	LET	CID OSI NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Loc LEA #1	Loc LEA #2	Loc LEA #3	St LEA	DOIM /IT	I	NEAR BASE	**Remarks**
PIR #1	**INSTALLATION**																					
1. WHAT LOCAL, REGIONAL, OR INTERNATIONAL ORGANIZATIONS POSE A POTENTIAL THREAT TO XXXX OR THE SURROUNDING COMMUNITY?				Always	Never	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	REPORTING REQUIREMENTS 1. LEC 111-111-1111 2. IOC 111-111-1111 3. CID 111-111-1111 4. MI 111-111-1111 5. OIS 111-111-1111 6. FBI 111-111-1111 (After Hrs 111-111-1111)
	1.1. WHAT MEANS DO THESE ORGANIZATIONS HAVE TO CONDUCT ATTACKS AGAINST XXXX AND THE SURROUNDING COMMUNITY?			Always	Never	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
		1.11. Information on purchase/theft of material to make improvised explosive devices	1.11a. Report unusual purchase/theft of explosives, weapons, ammo, HAZMAT, fertilizers, chemicals, etc.	Always	Never																	
		1.12. Information on purchase of large qualntity of weapons or theft of weapons	1.12a. Report unusual purchase/theft of vehicles capable of being configured with explosives and/or WMD	Always	Never																	
		1.13. Inofrmation on suspicious cars/trucks/vans activity	1.13a. Report on vehicles modified to handle heavier loads	Always	Never																	
		1.14. Information on suspicious activity dealing with military IDs, DOD decals, or other XXXX special access passes	1.14a. Report loss or stolen government vehicles or license plates	Always	Never																	
			1.14b. Report on purchase/theft of vehicles with DOD decals																			
			1.14c. Report loss/theft of military IDs or special access passes																			
		1.15. Information on unusual airborne activity on/vicinity XXXX	1.15a. Report unusual flight patterns of helicopters, single-engine aircraft, parachute/gliders, or parafoils																			
			1.15b. Report theft of airborne platforms																			
		1.16. Information on attempts to attack/access XXXX computer network	1.16a. Report any attempt to access XXXX computer network or reports of stolen/misused passwords																			
			1.16b. Report any ADP viruses immediately																			
			1.16c. Report any suspicious telephone calls or emails																			

Figure K-1. Installation Threat Information Organization Plan

INSTALLATION THREAT INFORMATION ORGANIZATION PLAN (cont'd)

				Collection		Collection Agencies																	
PIR	IR	Indicators	Specific Information Requirements (SIRs)	Date Info needed	Date info no longer needed	LET	CID OSI NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Loc LEA #1	Loc LEA #2	Loc LEA #3	St LEA	DOIM /IT	I	NEAR BASE	Remarks
PIR #1 (cont'd)	INSTALLATION																					
	1.2. WHAT HISTORICAL PATTERNS OF ATTACK HAS THIS GROUP EMPLOYED?			Always	Never																	
		1.21. Information on modus operandi of domestic dissident groups operating vicinity XXXX	1.21a. Report any suspicious activity associated with local domestic dissident groups	Always	Never																	
		1.22. Information on increase criminal activity on/vicinity XXXX	1.22a. Review records and report on previous activity of local domestic dissident groups	Always	Never																	
		1.23. Information on foreign terrorist groups, or groups sympathetic to foreign terrorist organizations, operating vicinity XXXX	1.23a. Report any suspicious activity associated foreign terrorist groups	Always	Never																	
		1.24. Increase in SAEDA reporting	1.24a. Review foreign terrorist modus operandi and report any suspicious activity that is similar	Always	Never																	
			1.24b. Report any former dissident members recently arrested/detained vicinity XXXX																			
	1.3. WHAT ARE THE RECENT ACTIVITIES OF THIS ORGANIZATION?			Always	Never																	
		1.31. Information on possible surveillance of XXXX	1.31a. Report all suspicious questions about XXXX or vicinity	Always	Never																	
		1.32. Information on possible unauthorized attempts to access XXXX	1.32a. Report all unauthorized attempts to access XXXX	Always	Never																	
		1.33. Queries about XXXX security measures	1.33a. Report all suspicious telephone calls or emails	Always	Never																	
		1.34. Requests for information on XXXX activities/missions/ memorandums of agreement (MOAs)/ memorandums of understanding (MOUs)	1.34a. Report all questions about sensitive locations																			
		1.35. Active dissident/ terrorist groups recruiting vicinity XXXX	1.35a. Report all questions about working relationships with local/state/federal law enforcement agencies																			
		1.36. Active dissident/ terrorist groups fund raising vicinity XXXX	1.36a. Report all suspicious request for job employment in vicinity XXXX																			

Figure K-1. Installation Threat Information Organization Plan (cont'd)

INSTALLATION THREAT INFORMATION ORGANIZATION PLAN (cont'd)

PIR	IR	Indicators	Specific Information Requirements (SIRs)	Collection		Collection Agencies																	Remarks
				Date Info needed	Date info no longer needed	LET	CID OSI NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Loc LEA #1	Loc LEA #2	Loc LEA #3	St LEA	DOIM /IT	I	NEAR BASE	
PIR #1 (cont'd)	**INSTALLATION**																						
		1.37. Active dissident/terrorist groups training vicinity XXXX	1.37a. Report all suspicious fund raising operations vicinity XXXX																				
			1.37b. Report all suspicious recruiting/training operations vicinity XXXX																				
			1.37c. Report what these groups collect against																				
		1.38. Recent arrests in the vicinity XXXX	1.38a. Report any suspicious individuals arrested/detained vicinity XXXX																				
	1.4. WHAT ADJUSTMENTS HAS THIS ORGANIZATION MADE IN RESPONSE TO CHANGES IN XXXX THREAT CONDITIONS AND FORCE PROTECTION CONDITIONS?			Always	Never																		
		1.41. Information on new methods dissident groups/terrorist organization are using to obtain information/surveil, recruit, fund raise, or acquire weapons/ equipment	1.41a. Report all suspicious questions about XXXX or vicinity	Always	Never																		
		1.42. Information on possible surveillance of XXXX	1.42a. Report all unauthorized attempts to access XXXX	Always	Never																		
		1.43. Information on possible unauthorized attempts to access XXXX	1.43a. Report all suspicious telephone calls or emails	Always	Never																		
		1.44. Queries about XXXX security measures	1.44a. Report all suspicious request for job employment in vicinity XXXX																				
			11. Report all suspicious recruiting/training operations vicinity XXXX																				
PIR #2	**INSTALLATION**																						
2. WHAT PATTERNS OF ACTIVITY, THREATS, OR LAW ENFORCEMENT ADVISORIES HAVE THERE BEEN THAT INDICATES AN INCREASED LIKELIHOOD OF ATTACK ON XXXX OR THE SURROUNDING COMMUNITY?																							

Figure K-1. Installation Threat Information Organization Plan (cont'd)

INSTALLATION THREAT INFORMATION ORGANIZATION PLAN (cont'd)

				Collection		Collection Agencies																
PIR	IR	Indicators	Specific Information Requirements (SIRs)	Date Info needed	Date info no longer needed	LET	CID OSI NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Loc LEA #1	Loc LEA #2	Loc LEA #3	St LEA	DOIM /IT	I	NEAR BASE	Remarks
PIR #2 (cont'd)	INSTALLATION																					
	2.1. HAVE THERE BEEN ANY SUSPICIOUS SURVEILLANCE ACTIVITIES ON XXXX OR AGAINST ASSIGNED PERSONNEL?																					
		2.11. Incidents of individuals videotaping, photographing, or sketching XXXX	2.11a. Report incidents of persons photographing, videoing, or sketching installation elements																			
		2.12. Incidents of unauthorized individuals attempting to access XXXX	2.12a. Report turn arounds at the gates																			
			2.12b. Report loss/theft of military IDs or special access passes																			
		2.13. Incidents of XXXX personnel being surveilled by suspicious personnel	2.13a. Report any suspicisous incidents where base personnel suspect they were being surveilled																			
		2.14. Unusual attempts to obtain military uniforms, DOD decals, military IDs or equipment in vicinity XXXX	2.14a. Report any attempts to obtain military uniforms or equipment																			
	2.2. HAVE THERE BEEN ANY THEFTS OF UNUSUAL CIRCUMSTANCE INVOLVING THE LOSS OF PERSONAL ID CARDS, VEHICLE REGISTRATION, GOVERNMENT LICENSE PLATES, OR GOVERNMENT VEHICLES.																					
		2.21. Incidents of stolen or lost personal ID cards	2.21a. Report loss or stolen government vehicles or license plates																			
		2.22. Incidents of stolen or lost DOD decals or special access passes for XXXX	2.22a. Report on purchase/theft of vehicles with DOD decals																			
		2.23. Incidents of stolen or lost government license plates	2.23a. Report loss/theft of military IDs or special access passes																			
		2.24. Incidents of stolen government vehicles	2.24a. Report all unauthorized attempts to access XXXX																			
		2.25. Increase in vehicle break-ins or car theft vicinity XXXX	2.25a. Report all attempts at vehicle break-ins or car theft vicinity XXXX																			

Figure K-1. Installation Threat Information Organization Plan (cont'd)

INSTALLATION THREAT INFORMATION ORGANIZATION PLAN (cont'd)

				Collection		Collection Agencies																
PIR	IR	Indicators	Specific Information Requirements (SIRs)	Date Info needed	Date info no longer needed	LET	CID OSI NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Loc LEA #1	Loc LEA #2	Loc LEA #3	St LEA	DOIM /IT	I	NEAR BASE	Remarks
PIR #2 (cont'd)	INSTALLATION																					
		2.26. Queries of unauthorized personnel attempting to obtain XXXX access passes	2.26a. Report all suspicious request for employment in vicinity XXXX																			
	2.3. HAVE THERE BEEN THEFTS OR UNUSUAL CIRCUMSTANCES INVOLVING THE LOSS OF PERSONAL OR GOVERNMENT WEAPONS, AMMUNITION, AND EXPLOSIVES.																					
		2.31. Increased reporting of theft of weapons, ammo, or explosive materials in vicinity XXXX	2.31a. Report unusual purchase/theft of explosives, weapons, ammo, HAZMAT, fertilizers, chemicals, etc.																			
		2.32. Attempts to illegally purchase weapons, ammunition, or explosive materials	2.32a. Report unusual purchase/theft of vehicles capable of being configured with explosives																			
		2.33. Unusual queries about location of storage of weapons on XXXX, particularly via telephone or email	2.33a. Report on vehicles modified to handle heavier loads																			
		2.34. Attempts of unauthorized individuals to observe military training sites where military weapons are utilized	2.34a. Report loss or stolen government vehicles or license plates																			
	2.4. HAVE THERE BEEN ANY PERIMETER VIOLATIONS, SECURITY BREECHES, UNAUTHORIZED INTRUSIONS, OR UNAUTHORIZED OVER-FLIGHTS OF XXXX?																					
		2.41. Incidents of physical signs of intrusion on XXXX	2.41a. Report loss or stolen government vehicles or license plates																			
		2.42. Incidents of unauthorized personnel attempting to access XXXX	2.42a. Report on purchase/theft of vehicles with DOD decals																			
		2.43. Incidents of unauthorized attempts to access XXXX	2.43.a. Report loss/theft of military IDs or special access passes, refused entries, or turn arounds at gate																			

Figure K-1. Installation Threat Information Organization Plan (cont'd)

FOR OFFICIAL USE ONLY

INSTALLATION THREAT INFORMATION ORGANIZATION PLAN (cont'd)

				Collection		Collection Agencies																		
PIR	IR	Indicators	Specific Information Requirements (SIRs)	Date Info needed	Date info no longer needed	LET	CID OSI NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Loc LEA #1	Loc LEA #2	Loc LEA #3	St LEA	DOIM /IT	I	NEAR BASE	Remarks
PIR #2 (cont'd)	INSTALLATION																					
	2.5. HAVE THERE BEEN RECEIPTS OF ANY SUSPICIOUS SHIPMENTS OF MAIL, PACKAGED FREIGHT, TRUCK INVENTORY, CONTAINERIZED SHIP CARGO, OR SPECIAL EQUIPMENT																					
		2.51. Increase in receipt of suspicious packages nation-wide	2.51a. Report any suspicious mail, packages, or cargo receive on/vicinity XXXX																			
		2.52. Increased reporting of potential threat to XXXX mail or cargo/shipments, especially by telephone or email.	2.52a. Report unusual purchase/theft of explosives, weapons, ammo, HAZMAT, fertilizers, chemicals, etc.																			
		2.53. Increase in stolen delivery/cargo/commercial trucks nation-wide, focus on vicinity XXXX	2.53a. Report unusual purchase/theft of vehicles capable of being configured with explosives																			
			2.54a. Report on vehicles modified to handle heavier loads																			
	2.6. HAVE THERE BEEN ANY THEFTS FROM SURROUNDING COMMUNITY OF COMMERCIAL AIRCRAFT, PRIVATE AIRCRAFT, COMMERCIAL OR PRIVATE HELICOPTERS, COMMERCIAL VEHICLES, TANKER TRUCK WITH A TANK CAPACITY OR MORE THAN 500 GALLONS OF BULK CHEMICAL, AND WATERCRAFT WITH A TANK CAPACITY OF MORE THAN 1000 GALLONS OF BULK CHEMICAL																					
		2.61. Increase reporting of threats against US facilities utilizing aircraft	2.61a. Report any threats against US facilities																			
			2.61b. Report incidents of unauthorized individuals attempting to gain access to aircraft																			
		2.62. Incidents of surveillance of airports, aircraft, hangars, or flight lines	2.62a. Report any incidents at airports.																			

Figure K-1. Installation Threat Information Organization Plan (cont'd)

INSTALLATION THREAT INFORMATION ORGANIZATION PLAN (cont'd)

PIR	IR	Indicators	Specific Information Requirements (SIRs)	Collection		Collection Agencies																Remarks
				Date Info needed	Date info no longer needed	LET	CID OSI NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Loc LEA #1	Loc LEA #2	Loc LEA #3	St LEA	DOIM /IT	I	NEAR BASE	
PIR #2 (cont'd)	**INSTALLATION**																					
		2.63. Incidents of thefts of aircraft, watercraft, or large trucks	2.63a. Report thefts of aircraft, watercraft, or large trucks																			
		2.64. Incidents of suspicious individuals trying to gain employment at businesses that have access to aircraft, commercial vehicles, tanker trucks, waterborne craft	2,64a. Report all suspicious attempts to gain employment with transportation industry in local area																			
PIR #3	**INSTALLATION**																					
3. WHAT EVENTS ARE TAKING PLACE ON XXXX OR IN THE SURROUNDING COMMUNITY THAT MAY PROVIDE AN OPPORTUNITY FOR A THREAT ATTACK?																						
	3.1. WHAT MAJOR SPORTING, CULTURAL, INDUSTRIAL, POLITICAL, MILITARY, OR OTHER SYMBOLIC EVENTS WILL TAKE PLACE AT XXXX OR IN THE COMMUNITY WITHIN THE NEXT 30 DAYS THAT MAY TRIGGER THE TARGETING INTERESTS OF THREAT ORGANIZATIONS?																					
		3.1.1. Unusual number of queries concerning events taking place on/vicinity XXXX	3.1.1a. Report any unusual questions about events taking place on/vicinity XXXX																			
		3.1.2. Increase number of reports nationally about threat to major sporting, cultural, industrial, political, military, or other symbolic events	3.1.2a. Report increase in threat reporting nation-wide concerning major sporting, cultural, industrial, political, military, or symbolic events																			
		3.1.3. Incidents of unauthorized individuals attempting to gain access to events on/vicinity XXXX	3.1.3a. Report all suspicious questions about XXXX or vicinity																			
		3.1.4. Incidents of individuals making queries about security measures pertaining to events on/vicinity XXXX	3.14a. Report all suspicious telephone calls or emails																			

Figure K-1. Installation Threat Information Organization Plan (cont'd)

INSTALLATION THREAT INFORMATION ORGANIZATION PLAN (cont'd)

				Collection		Collection Agencies																
PIR	IR	Indicators	Specific Information Requirements (SIRs)	Date Info needed	Date info no longer needed	LET	CID OSI NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Loc LEA #1	Loc LEA #2	Loc LEA #3	St LEA	DOIM /IT	I	NEAR BASE	Remarks
PIR #3 (cont'd)	**INSTALLATION**																					
		3.15. Incidents of suspicious individuals attempting to gain employment to support specific events on/vicinity XXXX	3.15a. Report suspicius attempts to gain employment at special events																			
	3.2. WHAT MOVEMENTS OF HAZARDOUS MATERIALS TAKE PLACE ON XXXX OR THE COMMUNITY THAT MAY TRIGGER THE TARGETING INTERESTS OF THREAT ORGANIZATIONS																					
		3.21. Incidents of individuals making queries about security measures pertaining to movements of hazardous materials within on/vicinity XXXX	3.21a. Report unusual queries concerning the movement of hazardous materials from XXXX																			
		3.22. Incidents of suspicious individuals trying to gain employment at businesses that have access to hazardous material	3.22a. Report unauthorized individuals attempting to gain access to XXXX																			
		3.23. Incidents of stolen vehicles designed or that can be configured to haul hazardous materials	3.23a. Report thefts or individuals making queries about security measures pertaining to the movement of hazardous materials on/vicinity XXXX																			
		3.24. Increase number of reports nationally about threat surrounding the use of hazardous materials	3.24a. Report news concerning the threat use of hazardous materials																			
PIR #4	**INSTALLATION**																					
4. DO INDICATORS EXIST OF A POSSIBLE INCIDENT AT XXXX OR THE SURROUNDING COMMUNITY INVOLVING NUCLEAR, BIOLOGICAL, OR CHEMCIAL WEAPONS?																						
	4.1. DO THREAT ORGANIZATIONS HAVE THE MEANS TO CONDUCT A NBC ATTACK OR A HAZARDOUS MATERIAL ATTACK AT XXXX OR IN THE SURROUNDING COMMUNITY?																					

Figure K-1. Installation Threat Information Organization Plan (cont'd)

INSTALLATION THREAT INFORMATION ORGANIZATION PLAN (cont'd)

PIR	IR	Indicators	Specific Information Requirements (SIRs)	Collection		Collection Agencies																Remarks
				Date Info needed	Date info no longer needed	LET	CID OSI NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Loc LEA #1	Loc LEA #2	Loc LEA #3	St LEA	DOIM /IT	I	NEAR BASE	
PIR #4 (cont'd)	INSTALLATION																					
		4.11. Incidents of stolen CBRNE material nationally and specifically in vicinity XXXX	4.11a. Report stolen CBRNE material in vicinity XXXX																			
		4.12. Incidents of unusual purchase of explosives, weapons, ammo, HAZMAT, fertilizers, chemicals, precursors, etc.	4.12a. Report excessive/unusual purchases of potential CBRNE material																			
		4.13. Incidents of unusual purchase/theft of vehicles capable of being configured with explosives/adapted for agent dissemination	4.13a. Report purchases of protective or lab equipment for agent handling																			
		4.14. Incidents of individuals making queries about security measures pertaining to CBRNE-related measures on/vicinity XXXX	4.14a. Report suspicious queries as to the capability of CBRNE materials																			
		4.15. Incidents of individuals making queries about security measures pertaining to CBRNE-related measures on/vicinity XXXX	4.15a. Report queries about the security of the chemicals utilized to train on XXXX																			
		4.16. Increased reporting of terrorist organization's ability and threat to use CBRNE material in the US	4.16a. Report unauthorized individuals attempting to gain access to XXXX																			
		4.17. Treatment for unusual illnesses or symptoms	4.17a. Report all medical cases seeking treatment for unusual illnesses or symptoms																			
		4.18. Purchase of CBRN antidotes	4.18a. Report purchases or attempted purchases of CBRN antidoes																			
			4.18b. Report any excess purchases of bleach																			
		4.19. Incidents of unusual odors or HAZMAT signs	4.19a. Report all cases of unusual odors or the appearance of HAZMAT signs																			
			4.19b. Report cases of unexplained animal deaths or lack of insect/plant life																			
	4.2. DO THESE THREAT ORGANIZATIONS HAVE A HISTORY OF CONDUCTING NBC ATTACKS?																					
		4.22. Past reporting of a terrorist group in vicinity XXXX utilizing CBRNE material to conduct attacks	4.22a. Review records and report on previous CBRNE activity of local domestic dissident groups																			

Figure K-1. Installation Threat Information Organization Plan (cont'd)

INSTALLATION THREAT INFORMATION ORGANIZATION PLAN (cont'd)

				Collection		Collection Agencies																	
PIR	IR	Indicators	Specific Information Requirements (SIRs)	Date Info needed	Date info no longer needed	LET	CID OSI NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Loc LEA #1	Loc LEA #2	Loc LEA #3	St LEA	DOIM /IT	I	NEAR BASE	Remarks
PIR #4 (cont'd)	INSTALLATION																					
	4.3. WHAT INDICATORS SUGGEST THAT A THREAT ORGANIZATION IS ABOUT TO CONDUCT AN ATTACK																					
		4.31. Incidents of threats to conduct CBRNE attacks in vicinity XXXX	4.31a. Report all related threats																			
		4.32. Incidents of stolen CBRNE materials in vicinity XXXX	4.32a. Report all stolen chemical agents																			
		4.33. Incidents of queries about XXXX's ability to respond to a CBRNE attack	4.33a. Report all suspicious inquiries about CBRN defense capabilities																			
		4.34. Incidents of unusual purchases of CBRNE protective gear	4.34a. Report thefts or purchases of CBRN protective gear																			
	4.4. WHERE ARE HAZARDOUS MATERIALS STORED, TRANSPORTED, OR USED IN BULK ON XXXX OR IN THE SURROUNDING COMMUNITY, WHICH COULD CREATE MASS CAUSALITIES?																					
		4.41. Chemical/ manufacturaing industries, water treatment, waste treatment facilities	4.41a. Report all suspicious activity at these locations or with their transportation assets																			
			4.41b. Report what chemicals and quantities are stored at these locations																			
			4.41c. Report how do these facilities store, receive, or ship chemicals																			
			4.41d. Report suspicious incidents related to storage or shipment of chemicals																			

Figure K-1. Installation Threat Information Organization Plan (cont'd)

INSTALLATION THREAT INFORMATION ORGANIZATION PLAN (cont'd)

ADP	automated data processing
ATF	Alcohol, Tobacco, and Firearms
CBRN	chemical, biological, radiological, and nuclear
CBRNE	chemical, biological, radiological, nuclear, and high-yield explosives
CI	counterintelligence
CID	Criminal Intelligence Division
CST	civil support team
DOD	Department of Defense
DOIM/IT	Department of Information Management/Information Technology staff
FBI	Federal Bureau of Investigation
HAZMAT	hazardous material
HHQ INT	higher headquarters intelligence
HS	homeland security
ID	identification
IR	information requirement
LE	law enforcement, military police, or security forces
LEA	law enforcement agency
LET	law enforcement team
Loc	local
NBC	nuclear, biological, and chemical
NCIS	Naval Criminal Investigation Service
OSI	Office of Special Investigations
PIR	priority information requirement
SAEDA	subversion and espionage against the US Army
SIR	specific information requirement
St	state
TWG	technical working group
WMD	weapons of mass destruction

Figure K-1. Installation Threat Information Organization Plan (cont'd)

APPENDIX L
HOMELAND SECURITY ADVISORY SYSTEM

1. Introduction

DHS maintains a HSAS to provide a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to Federal, state, and local authorities and to the American people. It provides warnings in the form of a set of graduated threat conditions that increase as the risk of the threat increases. At each threat condition, Federal departments and agencies implement a corresponding set of protective measures to further reduce vulnerability or increase response capability during a period of heightened alert.

2. Threat Conditions

a. There are five threat conditions, each identified by a description and corresponding color. From lowest to highest, the levels and colors are: low — green; guarded — blue; elevated — yellow; high — orange; and severe — red.

(1) Low — Green. This condition is declared when there is a low risk of terrorist attack.

(2) Guarded — Blue. This condition is declared when there is a general risk of terrorist attack.

(3) Elevated — Yellow. This condition is declared when there is increased surveillance.

(4) High — Orange. This condition is declared when there is a high risk of terrorist attack.

(5) Severe — Red. This condition is declared when there is a severe risk of terrorist attack.

b. There is no direct correlation between the HSAS and FPCON systems. The comparison provided in Figure M-1 is for information only.

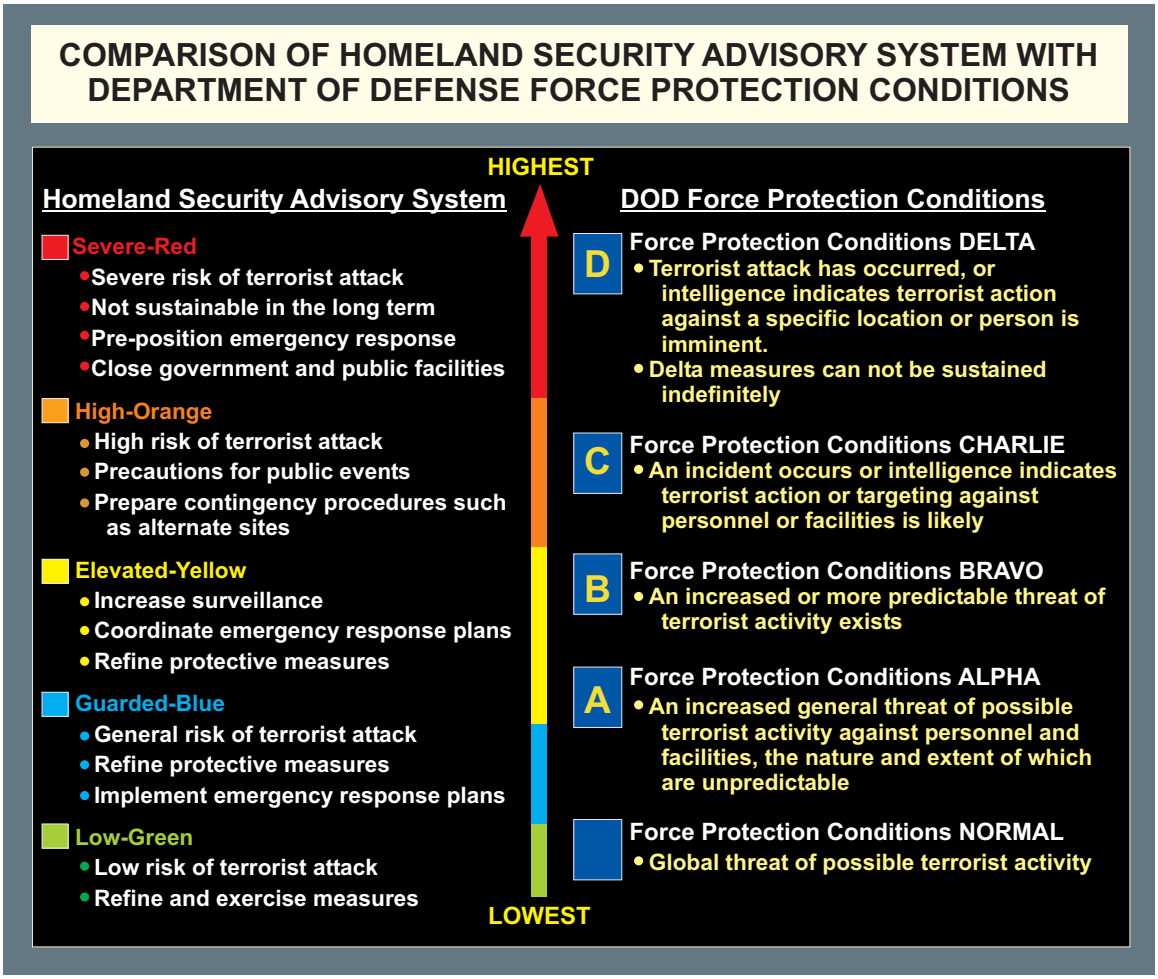


Figure L-1. Comparison of Homeland Security Advisory System with Department of Defense Force Protection Conditions

APPENDIX M
CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR DEFENSE PLANNING CONSIDERATIONS

1. Introduction

Originally developed to support warfighters, an overview of CBRN defense planning considerations is shown in Figure M-1. Sense, shape, shield, and sustain (i.e., the 4 S's) describe the fundamental concepts within CBRNE defense planning as part of AT.

2. Planning Considerations

a. "SENSE" is the capability to continually provide information about the CBRN situation at a time and place by detecting, identifying, and quantifying CBRN hazards in air, water, on land, on personnel, equipment, or facilities. This capability includes detecting, identifying, and quantifying those CBRN hazards in all physical states (solid, liquid, gas). "Sense" is the key enabler to help emergency responders assess and understand CBRN hazards.

(1) "Sense" procedures should detect and identify immediate CBRN hazards in the air; on mission-critical work areas and equipment; on personnel; in water, food, or soil; on equipment or facilities.

(2) "Sense" procedures should determine the extent of the hazard (based on available sensing equipment), support protection and mission planning decisions, and confirm operationally significant hazards have been removed, reduced, or eliminated.

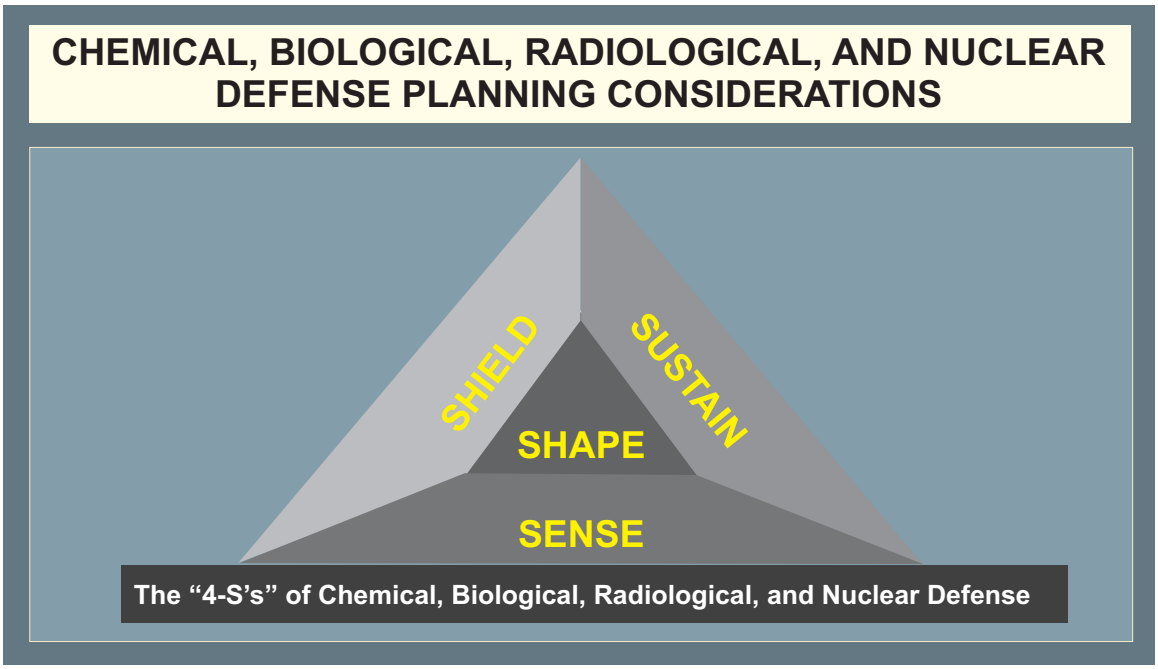


Figure M-1. Chemical, Biological, Radiological, and Nuclear Defense Planning Considerations

(3) Use sensors to monitor and warn of the presence of CBRN hazards at key points or critical missions on an installation, particularly during increased threat conditions. Selective CBRN sensor use, though, may be smarter than continuous around-the-clock monitoring.

b. "SHAPE" provides the ability to characterize the CBRN hazard for the force commander. "Shape" supports command decisions to protect personnel and continue critical missions.

(1) Develop a clear understanding of the current and predicted CBRN situation.

(2) Collect, query, and assimilate information from sensors, intelligence, medical, etc., in near real time.

(3) Inform personnel as appropriate of CBRN hazards.

(4) Provide actual and potential impacts of CBRN hazards.

(5) Envision critical SENSE, SHIELD, and SUSTAIN end states (preparation for operations).

(6) Visualize the sequence of events that moves the force from its current state to those end states.

c. "SHIELD" protects the force from harm caused by CBRN hazards by preventing or reducing individual and collective exposures, applying prophylaxis to prevent or mitigate negative physiological effects, and protecting critical equipment. The installation commander:

(1) Prevents or reduces CBRN casualties by reducing the threat, reducing operational vulnerability, and avoiding exposure.

(2) Provides appropriate levels of physical protection, medical treatment, or evacuation procedures to minimize casualties as possible (given equipment and treatment available).

(3) Must prepare to continue critical missions while minimizing potential CBRN hazard exposure.

(4) Relies on emergency responders through rapid response, assessment, and initial recovery operations.

(5) Takes steps to safeguard personnel from continued hazards, to control contamination, and to initiate steps to restore the area to its pre-incident conditions.

(6) Must coordinate with local, state, and regional emergency agencies to coordinate mutual assistance.

d. "SUSTAIN" includes actions to continue critical missions, respond appropriately, protect personnel, and restore combat power after a CBRN incident. Decontamination and medical actions, for example, enable an installation to facilitate a return to pre-incident operational capability as soon as possible.

(1) Depending on the operational impact of a CBRN incident, installation recovery efforts might be delayed in order to restore critical missions or essential operations.

(2) Crime scene and epidemiological investigations may also be needed.

(3) Eventually the installation should be restored to pre-incident operation capability levels.

(4) Emergency response, thorough decontamination, long-term remediation and recovery, and mortuary affairs must be coordinated with local, state, Federal (or HN) emergency response agencies. Installation commanders should integrate capabilities from external agencies in order to sustain continuous capabilities.

(5) Installation commanders must be prepared to transition from emergency response to Federal incident control and then back to DOD control during long-term restoration and recovery. Transitions must be done together with local, state, Federal, HN, and Service assets used in a military-civilian partnership.

Intentionally Blank

APPENDIX N
JOINT ANTITERRORISM PROGRAM MANAGER'S GUIDE

1. Introduction

a. The JAT Guide provides installation commanders, in transit commanders, and expeditionary commanders with the requirements, processes, tools, and templates to develop an effective AT program. The Guide provides DOD with a comprehensive and consistent planning capability to protect personnel and their families, installations, information, and other resources from a broad range of terrorist acts.

b. The guide operates on the installation's personal computers and guides the user through the correct steps and order using active 'subject buttons' and drop down menus. The JAT Guide is available for use online at www.atep.smil.mil and at https://atep.dtic.mil. Copies can also be ordered directly from JATGUIDE@ERCD.USACE.ARMY.MIL.

2. Joint Antiterrorism Guide Tools

a. The JAT Guide consists of four major modules that provide a 'how to' for AT planning, training, exercising, and reviewing that meet the requirements of DODI 2000.16, *DOD Antiterrorism Standards*. JAT Guide works through the risk management process and accesses technical defense.

b. Several major analysis and decision aid tools are also included or accessed through the Guide:

(1) JAT Database.

(2) JAT Graphics.

(3) AT Planner.

(4) Window Fragment Hazard Level Analysis.

(5) Hazard Prediction and Assessment Capability.

(6) Vulnerability Assessment Management Program.

(7) Flight Path Threat Analysis Simulation.

c. Templates are also included to tabulate, analyze, and display information to support the process and tools.

Intentionally Blank

APPENDIX O
REFERENCES

The development of JP 3-07.2 is based upon the following primary references:

1. Presidential Military Order of November 13, 2001, *Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism*.

2. Public Law 107–314—Dec. 2, 2002, *Bob Stump National Defense Authorization Act for Fiscal Year 2003*.

3. Public Law 107–296—Nov. 25, 2002, *Homeland Security Act of 2002*.

4. Statement by Mr. Paul McHale, Assistant Secretary of Defense for Homeland Defense Before the 108th Congress Senate Armed Services Committee US Senate April 8, 2003.

5. United States Department of State, *Patterns of Global Terrorism 2003, April 2004.*

6. DOD Military Commission Order No. 1, *Procedures for Trials by Military Commissions of Certain Non-United States Citizens in the War on Terrorism*.

7. *National Strategy for Combating Terrorism*, February 2003.

8. *National Security Strategy of the United States of America,* September 2002.

9. *National Strategy for Homeland Security*, July 2002.

10. *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets,* February 2003.

11. *The US Coast Guard Maritime Strategy for Homeland Security*, December 2002.

12. Statements for the Record of Assistant Directors of the Federal Bureau of Investigation before House Committees and Subcommittees of the US Congress.

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

14. *Operational Law Handbook (2003)*.

15. DODD 2000.12, *DOD Antiterrorism (AT) Program*.

16. DOD O-2000.12-H, *DOD Antiterrorism Handbook*, 9 February 2004.

17. DODD 3020.40, *Defense Critical Infrastructure Program (DCIP)*.

18. DODD 3025.1, *Military Support to Civil Authorities (MSCA)*.

19. DODD 3025.12, *Military Assistance for Civil Disturbances (MACDIS)*.

20. DODD 3025.15, *Military Assistance to Civil Authorities*.

21. DODD 4500.54, *Official Temporary Duty Travel Abroad*.

22. DODD 4500.54-G, *DOD Foreign Clearance Guide (FCG)*.

23. DODD 5105.62, *Defense Threat Reduction Agency.*

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

25. DODD 5240.1, *DOD Intelligence Activities*.

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

27. DODD 5525.5, *DOD Cooperation with Civilian Law Enforcement Officials*.

28. DODD 5525.7, *Implementation of the Memorandum of Understanding Between the Department of Justice and the Department of Defense Relating to the Investigation and Prosecution of Certain Crimes*.

29. DODI 2000.14, *DOD Combating Terrorism Program Procedures*.

30. DODI 2000.16, *DOD Antiterrorism Standards*.

31. DODI 3020.41, *Contractor Personnel Authorized to Accompany the US Armed Forces*.

32. DODI 5240.6, *Counterintelligence (CI) Awareness, Briefing, and Reporting Programs*.

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

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

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

36. JP 3-05, *Doctrine for Joint Special Operations*.

37. JP 3-08, *Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations*.

38. JP 3-10, *Joint Security Operations in Theater*.

39. JP 3-16, *Joint Doctrine for Multinational Operations*.

40. JP 3-26, *Homeland Security*.

41. JP 3-40, *Joint Doctrine for Combating Weapons of Mass Destruction*.

42. JP 3-54, *Operations Security*.

43. CJCSI 3121.01B, *Standing Rules of Engagement for US Forces (U)*.

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

45. CJCSI 5261.01D, *Combating Terrorism Readiness Initiatives Fund*.

46. Chairman of the Joint Chiefs of Staff Manual 3122.03A, *Joint Operation Planning and Execution System Vol II: (Planning Formats and Guidance)*.

47. Director of Central Intelligence Memorandum, Homeland Security Information Sharing Memorandum of Understanding, 4 March 2003 (DAC-01355-03).

48. Deputy Security of Defense Memorandum, Collection, Reporting, and Analysis of Terrorist Threats to DOD Within the United States, 2 May 2003 (U05646-03).

49. FM 3-11.21 (Army), MCRP 3-37.2C (USMC), NTTP 3-11.24 (Navy), and AFTTP (I) 3-2.37 (USAF), *Multi-Service Tactics, Techniques, and Procedures for Nuclear, Biological, and Chemical Aspects of Consequence Management*.

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

51. TM 5-853, AFMAN 32-1071, *Security Engineering*.

52. FM 5-114, *Engineer Operations Short of War*.

Intentionally Blank

APPENDIX P
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

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

2. Authorship

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

3. Supersession

This publication supersedes JP 3-07.2, 17 March 1998, *Joint Tactics, Techniques, and Procedures for Antiterrorism*.

4. Change Recommendations

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

TO: JOINT STAFF WASHINGTON DC//J34//
INFO: JOINT STAFF WASHINGTON DC//J7-JEDD//
CDRUSJFCOM SUFFOLK VA//DOC GP//

Routine changes should be submitted electronically to Commander, Joint Warfighting Center, Doctrine and Education Group and info the Lead Agent and the Director for Operational Plans and Joint Force Development J-7/JEDD via the CJCS JEL at http://www.dtic.mil/doctrine.

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

c. Record of Changes:

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

5. Distribution of Printed Publications

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

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

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

By Military Services:

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

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

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

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

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

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

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

6. Distribution of Electronic Publications

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

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

Intentionally Blank

GLOSSARY

PART I — ABBREVIATIONS AND ACRONYMS

ACP	access control point
AFMAN	Air Force manual
AFOSI	Air Force Office of Special Investigations
AMC	Air Mobility Command
AOR	area of responsibility
ASD(HD)	Assistant Secretary of Defense (Homeland Defense)
ASD(SO/LIC)	Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict)
AT	antiterrorism
ATCC	Antiterrorism Coordinating Committee
ATCC-SSG	Antiterrorism Coordinating Committee-Senior Steering Group
ATEP	Antiterrorism Enterprise Portal
ATO	antiterrorism officer
ATWG	antiterrorism working group
C2	command and control
CARVER	criticality, accessibility, recuperability, vulnerability, effect, and recognizability
CBRN	chemical, biological, radiological, and nuclear
CBRNE	chemical, biological, radiological, nuclear, and high-yield explosives
CbT	combating terrorism
CbT-RIF	Combating Terrorism Readiness Initiatives Fund
CI	counterintelligence
CIA	Central Intelligence Agency
CIFA	Counterintelligence Field Activity
CISD	critical incident stress debriefing
CISO	counterintelligence staff officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CM	consequence management
COM	chief of mission
CONUS	continental United States
COOP	continuity of operations
CT	counterterrorism
CVAMP	Core Vulnerability Assessment Management Program
DBT	design basis threat
DCIP	Defense Critical Infrastructure Program
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DOD	Department of Defense

DODD	Department of Defense directive
DODI	Department of Defense instruction
DOJ	Department of Justice
DOS	Department of State
DSS	Defense Security Service
DTA	Defense Threat Assessment
DTAM	defense terrorism awareness message
DTRA	Defense Threat Reduction Agency
DVD	digital video disc
ECP	entry control point
EO	executive order
EOC	emergency operations center
EOD	explosive ordnance disposal
EXECSEC	executive secretary
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FM	field manual (Army)
FP	force protection
FPCON	force protection condition
FPTAS	flight path threat analysis simulation
FRF	fragment retention film
HAZMAT	hazardous material
HD	homeland defense
HE	high explosive
HN	host nation
HNS	host-nation support
HQ	headquarters
HRB	high-risk billet
HRP	high-risk personnel
HS	homeland security
HSAS	Homeland Security Advisory System
ICS	incident command system
IED	improvised explosive device
IGO	intergovernmental organization
IO	information operations
IR	information requirement
IRF	incident response force
ISR	intelligence, surveillance, and reconnaissance

J-2	intelligence directorate of a joint staff
J-3	operations directorate of a joint staff
JAT Guide	Joint Antiterrorism Program Manager's Guide
JFC	joint force commander
JITF-CT	Joint Intelligence Task Force for Combating Terrorism
JP	joint publication
JRA	joint rear area
JSC	joint security coordinator
JSIVA	Joint Staff Integrated Vulnerability Assessment
JTF	joint task force
JTTF	joint terrorism task force
LE	law enforcement
LFA	lead federal agency
LOC	line of communications
LOS	line of sight
LP	listening post
MANPADS	man-portable air defense system
MEVA	mission essential vulnerable area
MOA	memorandum of agreement
MOU	memorandum of understanding
MSHARPP	mission, symbolism, history, accessibility, recognizability, population, and proximity
MWD	military working dog
NCIS	Naval Criminal Investigative Service
NG	National Guard
NGO	nongovernmental organization
NIMS	National Incident Management System
NRP	National Response Plan
OASD(PA)	Office of the Assistant Secretary of Defense (Public Affairs)
OC	operations center
OCONUS	outside the continental United States
OIF	Operation IRAQI FREEDOM
OP	observation post
OPLAN	operation plan
OPSEC	operations security
OSD	Office of the Secretary of Defense
PA	public affairs
PAO	public affairs officer
PCA	Posse Comitatus Act
PIR	priority intelligence requirement

POM	program objective memorandum
PPBE	Planning, Programming, Budgeting, and Execution
PSYOP	psychological operations
R&R	rest & recuperation
RA	risk assessment
RAM	random antiterrorism measure
ROE	rules of engagement
RUF	rules for the use of force
SAR	suspicious activity report
SecDef	Secretary of Defense
SECSTATE	Secretary of State
SES	senior executive service
SIPRNET	SECRET Internet Protocol Router Network
SIR	specific information requirement
SJA	staff judge advocate
SOC	security operations center
SOFA	status-of-forces agreement
SOP	standing operating procedure
TA	threat assessment
TACON	tactical control
TALON	Threat and Local Observation Notice
TIM	toxic industrial material
TM	technical manual
TTG	thermally tempered glass
TTP	tactics, techniques, and procedures
UFC	Unified Facilities Criteria
UFR	unfunded requirement
USACIDC	United States Army Criminal Investigation Command
USC	United States Code
USCG	United States Coast Guard
USG	United States Government
USNORTHCOM	United States Northern Command
VA	vulnerability assessment
VBIED	vehicle borne improvised explosive device
WMD	weapons of mass destruction

PART II — TERMS AND DEFINITIONS

aircraft piracy. None. (Approved for removal from the next edition of JP 1-02.)

antiterrorism. Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces. Also called AT. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

antiterrorism awareness. None. (Approved for removal from the next edition of JP 1-02.)

chemical, biological, radiological, and nuclear defense. Efforts to protect personnel on military installations and facilities from chemical, biological, radiological, and nuclear incidents. Also called CBRN defense. (Approved for inclusion in the next edition of JP 1-02.)

chemical, biological, radiological, nuclear, and high-yield explosive hazards. Those chemical, biological, radiological, nuclear, and high-yield explosive elements that pose or could pose a hazard to individuals. Chemical, biological, radiological, nuclear, and high-yield explosive hazards include those created from accidental releases, toxic industrial materials (especially air and water poisons), biological pathogens, radioactive matter, and high-yield explosives. Also included are any hazards resulting from the deliberate employment of weapons of mass destruction during military operations. Also called CBRNE hazards. (Approved for inclusion in the next edition of JP 1-02.)

chief of mission. A chief of mission (COM) (normally the ambassador) is the principal officer in charge of a diplomatic facility of the United States, including any individual assigned to be temporarily in charge of such a facility. The COM is the personal representative of the President to the country of accreditation. The COM is responsible for the direction, coordination, and supervision of all US Government executive branch employees in that country (except those under the command of a US area military commander). The security of the diplomatic post is the COM's direct responsibility. Also called COM. (JP 1-02)

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

combating terrorism. Actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), taken to oppose terrorism throughout the entire threat spectrum. Also called CbT. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

consequence management. Actions taken to maintain or restore essential services and manage and mitigate problems resulting from disasters and catastrophes, including natural, manmade, or terrorist incidents. Also called CM. (JP 1-02)

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

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

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

criticality assessment. An assessment that identifies key assets and infrastructure that support Department of Defense missions, units, or activities and are deemed mission critical by military commanders or civilian agency managers. It addresses the impact of temporary or permanent loss of key assets or infrastructures to the installation or a unit's ability to perform its mission. It examines costs of recovery and reconstitution including time, dollars, capability, and infrastructure support. (Approved for inclusion in the next edition of JP 1-02.)

design basis threat. The threat against which an asset must be protected and upon which the protective system's design is based. It is the baseline type and size of threat that buildings or other structures are designed to withstand. The design basis threat includes the tactics aggressors will use against the asset and the tools, weapons, and explosives employed in these tactics. Also called DBT. (Approved for inclusion in the next edition of JP 1-02.)

deterrence. The prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction. (JP 1-02)

force protection. Actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease. Also called FP. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

force protection condition. A Chairman of the Joint Chiefs of Staff-approved program standardizing the Military Services' identification of and recommended responses to terrorist threats against US personnel and facilities. This program facilitates inter-Service coordination. Also called FPCON. There are four FPCONs above normal. a. FPCON ALPHA — This condition applies when there is an increased 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 FPCON BRAVO measures. However, it may be necessary to implement certain measures from higher FPCONs resulting from intelligence received or as a deterrent. The measures in this FPCON

must be capable of being maintained indefinitely. b. FPCON BRAVO — This condition applies when an increased or more predictable threat of terrorist activity exists. Sustaining the measures in this FPCON for a prolonged period may affect operational capability and relations with local authorities. c. FPCON CHARLIE — This condition applies when an incident occurs or intelligence is received indicating some form of terrorist action or targeting against personnel or facilities is likely. Prolonged implementation of measures in this FPCON may create hardship and affect the activities of the unit and its personnel. d. FPCON 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 imminent. Normally, this FPCON is declared as a localized condition. FPCON DELTA measures are not intended to be sustained for substantial periods. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

high-risk personnel. Personnel who, by their grade, assignment, symbolic value, or relative isolation, are likely to be attractive or accessible terrorist targets. Also called HRP. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

homeland defense. The protection of United States sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression or other threats as directed by the President. The Department of Defense is responsible for homeland defense. Homeland defense includes missions such as domestic air defense. The Department recognizes that threats planned or inspired by "external" actors may materialize internally. The reference to "external threats" does not limit where or how attacks could be planned and executed. The Department is prepared to conduct homeland defense missions whenever the President, exercising his constitutional authority as Commander in Chief, authorizes military actions. Also called HD. (JP 1-02)

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

hostage. A person held as a pledge that certain terms or agreements will be kept. (The taking of hostages is forbidden under the Geneva Conventions, 1949). (JP 1-02)

improvised explosive device. A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. It may incorporate military stores, but is normally devised from nonmilitary components. Also called IED. (JP 1-02)

information operations. The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own. Also called IO. (JP 1-02)

initial response force. The first unit, usually military police, on the scene of a terrorist incident. (JP 1-02)

installation. A grouping of facilities, located in the same vicinity, which support particular functions. Installations may be elements of a base. (JP 1-02)

installation commander. The individual responsible for all operations performed by an installation. (JP 1-02)

insurgent. Member of a political party who rebels against established leadership. (JP 1-02)

intelligence. 1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (JP 1-02)

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

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

operations center. The facility or location on an installation, base, or facility used by the commander to command, control, and coordinate all operational activities. Also called OC. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

operations security. 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 that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. (JP 1-02)

physical security. 1. 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. 2. In

communications security, the component that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (JP 1-02)

prevention. 1. The security procedures undertaken by the public and private sectors in order to discourage terrorist acts. (JP 1-02)

primary target. None. (Approved for removal from the next edition of JP 1-02.)

proactive measures. In antiterrorism, measures taken in the preventive stage of antiterrorism designed to harden targets and detect actions before they occur. (JP 1-02)

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

risk. 1. Probability and severity of loss linked to hazards. (JP 1-02)

risk assessment. The identification and assessment of hazards (first two steps of risk management process). Also called RM. (JP 1-02)

risk management. The process of identifying, assessing, and controlling, risks arising from operational factors and making decisions that balance risk cost with mission benefits. (JP 1-02)

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

secondary targets. None. (Approved for removal from the next edition of JP 1-02.)

status-of-forces agreement. An agreement that defines the legal position of a visiting military force deployed in the territory of a friendly state. Agreements delineating the status of visiting military forces may be bilateral or multilateral. Provisions pertaining to the status of visiting forces may be set forth in a separate agreement, or they may form a part of a more comprehensive agreement. These provisions describe how the authorities of a visiting force may control members of that force and the amenability of the force or its members to the local law or to the authority of local officials. To the extent that agreements delineate matters affecting the relations between a military force and civilian authorities and population, they may be considered as civil affairs agreements. Also called SOFA. (JP 1-02)

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. (JP 1-02.)

terrorist. An individual who commits an act or acts of violence or threatens violence in pursuit of political, religious, or ideological objectives. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

terrorist group. Any number of terrorists who assemble together, have a unifying relationship, or are organized for the purpose of committing an act or acts of violence or threatens violence in pursuit of their political, religious, or ideological objectives. (This term and its definition modify the existing term "terrorist groups" and its definition and are approved for inclusion in the next edition of JP 1-02.)

terrorist threat level. An intelligence threat assessment of the level of terrorist threat faced by US personnel and interests in a foreign country. The assessment is based on a continuous intelligence analysis of a minimum of five elements: terrorist group existence, capability, history, trends, and targeting. There are five threat levels: NEGLIGIBLE, LOW, MEDIUM, HIGH, and CRITICAL. Threat levels should not be confused with force protection conditions. Threat level assessments are provided to senior leaders to assist them in determining the appropriate local force protection condition. (The Department of State also makes threat assessments, which may differ from those determined by Department of Defense.) (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

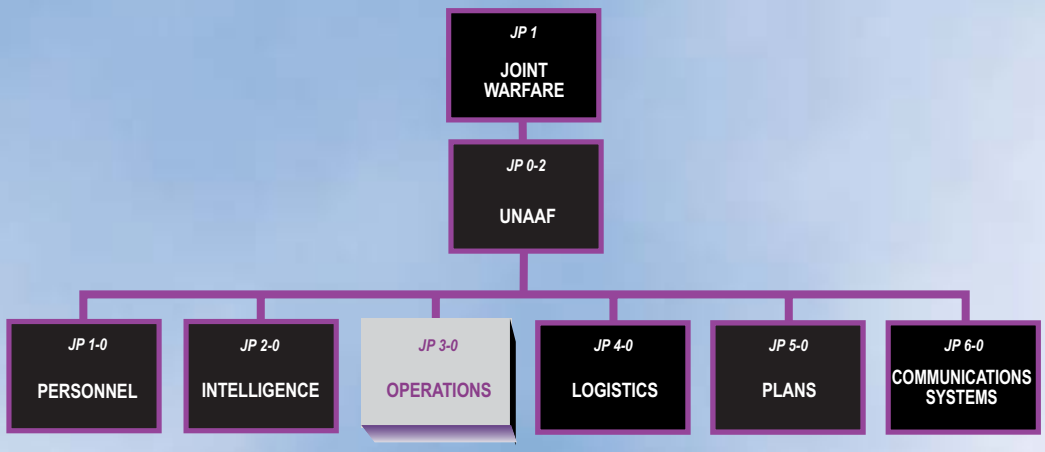
threat analysis. In antiterrorism, a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups which could target a facility. A threat analysis will review the factors of a terrorist group's existence, capability, intentions, history, and targeting, as well as the security environment within which friendly forces operate. Threat analysis is an essential step in identifying probability of terrorist attack and results in a threat assessment. (JP 1-02)

threat and vulnerability assessment. In antiterrorism, the pairing of a facility's threat analysis and vulnerability analysis. (JP 1-02)

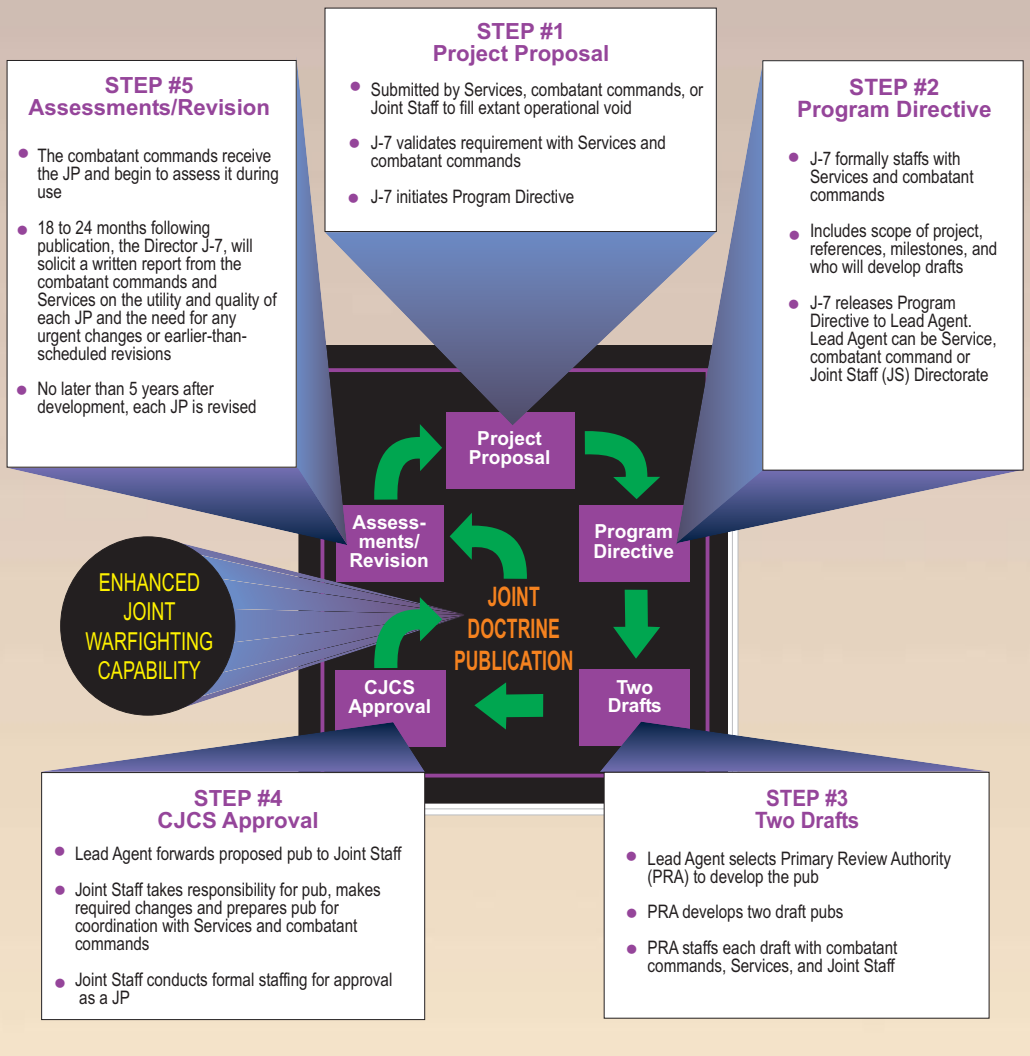
vulnerability assessment. A Department of Defense, command, or unit-level evaluation (assessment) to determine the vulnerability of a terrorist attack against an installation, unit, exercise, port, ship, residence, facility, or other site. Identifies areas of improvement to withstand, mitigate, or deter acts of violence or terrorism. Also called VA. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

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

JOINT DOCTRINE PUBLICATIONS HIERARCHY



All joint doctrine is organized into a comprehensive hierarchy as shown in the chart above. **Joint Publication (JP) 3-07.2** is in the **Operations** series of joint doctrine publications. The diagram below illustrates an overview of the development process:




JOINT
CHIEFS OF STAFF