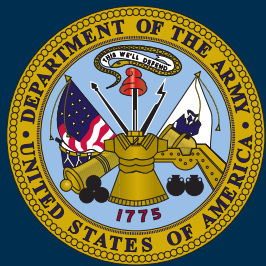


Joint Publication 3-07.2



Antiterrorism



24 November 2010



Intentionally Blank

PREFACE

1. Scope

This publication provides joint doctrine for planning, executing, and assessing 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 joint 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, education, 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 Joint Staff, 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:

A handwritten signature in black ink, appearing to be 'W E GORTNEY', written in a stylized, cursive-like font.

WILLIAM E. GORTNEY
VADM, USN
Director, Joint Staff

Intentionally Blank

SUMMARY OF CHANGES
REVISION OF JOINT PUBLICATION 3-07.2
DATED 14 APRIL 2006

- **Removes all “For Official Use Only” information.**
- **Changes the definitions of “terrorism” and “antiterrorism” and explains the difference between “terrorism” and “insurgency.”**
- **Provides greater depth on terrorist structures, categories, and affiliations. Also adds a discussion on “lone terrorists.”**
- **Adds the use of “improvised explosive devices,” “explosively formed projectiles,” and “suicide bombing” in terrorist tactics.**
- **Updates the capabilities and functions of several intelligence and law enforcement organizations, including resources for obtaining intelligence relevant to the commander.**
- **Adds a discussion on “Countering Terrorist Attack Planning,” to include details on “the terrorist attack planning cycle,” “surveillance detection,” and “surveillance awareness.”**
- **Removes a chapter on "Preventive Measures and Considerations" and moves its contents to the other chapters.**
- **Combines four separate risk-management-related appendices into one "Risk Management" Appendix.**
- **Removes five other appendixes with information that is better covered and more up to date in other publications, to include: “Sample Barrier Plan,” “FPCON system,” “Homeland Security Advisory System,” “CBRN Planning Considerations,” and “JAT Program Manager's Guide.”**

Intentionally Blank

TABLE OF CONTENTS

	PAGE
EXECUTIVE SUMMARY	vii
CHAPTER I	
INTRODUCTION	
• General Operational Context	I-1
• Antiterrorism in the Context of Other Protection Efforts	I-2
• Overview of Antiterrorism Program.....	I-3
• Overview of Department of Defense Roles and Responsibilities	I-3
CHAPTER II	
TERRORIST THREAT	
• Threat of Terrorism.....	II-1
• Terrorist Organizational Structures	II-1
• Lone Terrorist	II-3
• Identity Based Terrorism	II-3
• State Affiliation	II-7
• Terrorist Membership	II-8
• Common Terrorist Tactics, Techniques, and Procedures	II-10
• Terrorist Use of Asymmetrical Tactics.....	II-12
• Terrorism Against the Homeland	II-15
CHAPTER III	
INTELLIGENCE	
• Role of Intelligence.....	III-1
• Intelligence and Risk Management	III-3
• Intelligence Support.....	III-4
• Antiterrorism Intelligence Roles and Responsibilities	III-8
CHAPTER IV	
LEGAL CONSIDERATIONS	
• General.....	IV-1
• Commander's Authority	IV-1
• Limits of Civil Support.....	IV-1
• Authority for Handling Terrorist Incidents.....	IV-2
• United States Coast Guard.....	IV-5

CHAPTER V

ANTITERRORISM PROGRAMS

- Antiterrorism Program Overview V-1
- Antiterrorism Plan Development V-3
- Countering Terrorist Attack Planning V-6

CHAPTER VI

TERRORIST INCIDENT RESPONSE

- General VI-1
- Incident Management Planning VI-1
- Initial Response VI-2
- Initial Response to a Chemical, Biological, Radiological, or Nuclear Attack VI-3
- Special Considerations VI-4
- Considerations in the United States VI-7

APPENDIX

- A Antiterrorism Plan A-1
- B Antiterrorism Checklist for Commanders and Antiterrorism Officers B-1
- C Threat Information Organization Matrix C-1
- D Preventive Measures and Considerations D-1
- E Risk Management Process E-1
- F References F-1
- G Administrative Instructions G-1

GLOSSARY

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

FIGURE

- I-1 Elements of Combating Terrorism I-2
- I-2 Antiterrorism Relationship to Force Protection I-4
- I-3 Antiterrorism Enterprise Portal I-8
- II-1 Terrorist State Affiliation II-7
- III-1 Sources of Intelligence III-5
- III-2 Information Requirements III-12
- V-1 Department of Defense Threat Level and Force Protection Conditions ... V-5
- V-2 Terrorist Attack Planning Cycle V-6
- V-3 Surveillance Indicators V-10
- C-1 Installation Threat Information Organization Plan C-2
- E-1 Notional Assessing Terrorist Threat Capability Threat/Priority Matrix .. E-13
- E-2 Example Asset Risk Assessment Table E-17
- E-3 Example of Risk Assessment E-19

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

Terrorists pose a grave danger to the national security and interests of the United States at home and abroad.

The National Strategy for Combating Terrorism outlines a strategic vision built around an international effort aimed at the defeat of violent extremism which threatens the way of life for free and open societies and creation of a global environment inhospitable to violent extremists and their supporters. Although there is no universal definition for terrorism, the Department of Defense (DOD) defines it as the unlawful use of violence or threat of violence to instill fear and coerce governments or societies. Terrorism is often motivated by religious, political, or other ideological beliefs and committed in the pursuit of goals that are usually political.

The broader construct of combating terrorism (CbT) is defined as actions, including antiterrorism (AT) and counterterrorism, taken to oppose terrorism throughout the entire threat spectrum.

Historically, **combating terrorism (CbT)** has been both a battle of arms and ideas—a fight against the terrorists and the ideology which drives terrorism. CbT remains an approach with both defensive and offensive components: antiterrorism (AT)—defined as **defensive measures used to reduce the vulnerability of individuals and property to terrorists acts, to include rapid containment by local military and civilian forces;** and counterterrorism—defined as **actions taken directly against terrorists networks and indirectly to influence and render global and regional environments inhospitable to terrorist networks.**

AT is one of several requirements under a commander's overall responsibility to provide protection.

As required or directed, the protection of forces, including the use of AT programs, may be extended to encompass protection of US noncombatants; the forces, systems, and civil infrastructure of friendly nations; and other government agencies, intergovernmental organizations, and nongovernmental organizations.

AT is not only a sub-element of CbT, but it is also a subset of the broader force protection construct.

Force protection (FP) is defined as preventive measures to mitigate hostile actions against DOD personnel (to include family members), resources, facilities, and critical information. FP does not include actions to defeat the enemy or protect against accidents, weather, or disease. While AT programs also integrate various FP-related programs to protect against terrorist attacks (physical security, chemical, biological, radiological, and nuclear [CBRN] passive defense, operations security [OPSEC], counterintelligence [CI], biometrics, and surveillance detection, etc.), it does not include all aspects of FP.

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 associated infrastructure critical to mission accomplishment as well as the preparations to defend against and plan for the response to the consequences of terrorist incidents. The minimum elements of an AT program are: risk management; planning; training and exercises; resource management; public awareness; and comprehensive program review.

Department of Defense (DOD) roles and responsibilities.

Policy. The DOD components, elements, and personnel shall be protected from terrorist acts through a high priority, comprehensive AT program using an integrated systems approach. Commanders should ensure the AT awareness and readiness of all DOD elements and personnel (including dependent family members) assigned or attached. The geographic combatant commanders' (GCCs') AT policies take precedence over all AT policies or programs of any DOD component operating or existing in that GCC's area of responsibility (AOR) except for those under the security responsibility of a chief of mission (COM).

Responsibilities.

Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD[HD&ASA]) provides overall supervision of AT, homeland defense

(HD), Defense Critical Infrastructure Program, and civil support activities within DOD.

The Secretaries of the Military Departments have the following responsibilities: institute and support AT programs in accordance with DOD Directive (DODD) 2000.12, *DOD Antiterrorism (AT) Program*; provide AT resident training to personnel assigned to high-risk billets and others as appropriate; ensure military construction programming policies include AT protective features for facilities and installations; provide a representative as a member of the DOD Antiterrorism Coordinating Committee and subcommittees, as required; ensure all assigned military, DOD civilians, DOD contractors, and their family members receive applicable AT training and briefings pursuant to DOD Instruction 2000.16, *DOD Antiterrorism (AT) Standards*.

Chairman of the Joint Chiefs of Staff serve as the principal advisor to the Secretary of Defense (SecDef) for all DOD AT issues; assess the implementation of force protection conditions for uniform implementation and dissemination; coordinate with the Under Secretary of Defense for Intelligence and the ASD(HD&ASA) on sharing of terrorism intelligence and CI data and information on AT; and maintain the Antiterrorism Enterprise Portal.

GCCs have overall AT responsibility within their AOR, except for those DOD elements and personnel for whom a COM has security responsibility pursuant to law or a memorandum of agreement (MOA). Exercise tactical control (TACON) for FP over all DOD elements and personnel (including DOD dependents, except those under the security responsibility of a COM) within the GCC's AOR. TACON (for FP) applies to all DOD personnel assigned, permanently or temporarily, transiting through, or performing exercises or training in the GCC's AOR.

Functional combatant commanders 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.

Directors of other DOD agencies and components support GCCs as they execute their AT programs. Institute AT programs of their own which include vulnerability assessments and contingency response plans.

Terrorist Threat

Terrorists use violence or the threat of violence to impact multiple audiences.

The current terrorist paradigm involves a broad spectrum of threats including traditional state-sponsored terrorism, networks of non-state actors, extremist groups, criminal networks, and radicalized individuals acting alone. A critical factor in understanding terrorism is the importance of the emotional and psychological impact of terrorism.

A general knowledge of prevalent terrorist organizational structures helps to understand their capabilities and the type of threat they pose.

A terrorist organization's structure, along with membership, resources, and security determine in part its capabilities, influence, and reach. Terrorist groups, regardless of ideology, location, or structure, have some common basic organizational imperatives: the need to survive and to pursue the goals of the organization, while remaining credible to their followers.

There are two typical organizational structures used by terrorist groups: hierarchical and networked.

Newer groups tend to organize or adapt to the networked model, while others associated with political organizations prefer the more centralized control of the hierarchical structure to coordinate violent action with political action. Most groups are composed of both structures, continuously adapting as the strategic environment dictates. Within either of those two larger organizational structures, however, virtually all terrorist groups organize as smaller cells at the tactical level.

Hierarchical Structure.

These organizations have a well-defined vertical chain of command and responsibility. Information flows up and down organizational channels that correspond to these vertical chains, but may not move horizontally through the organization. Hierarchies are traditional and common of larger groups that are well established with a command and support structure. Hierarchical organizations feature greater specialization of functions in their subordinate cells (support, operations, intelligence).

Networked Structure.

Unlike hierarchies, networks distribute authority and responsibility throughout an organization, often creating redundant key functions. To be effective, networks require a unifying idea, concern, goal, or ideology.

Without a unifier, networks may take actions that are counterproductive, and independent nodes may not develop the necessary cohesiveness for success of the network. General goals and targets are announced, and individuals or cells with redundant capabilities are expected to use flexibility and initiative to conduct the necessary actions.

There are three basic types of network structures, depending on the ways in which elements (nodes) are linked to other elements of the structure: the chain, hub (or spoke and wheel), and all-channel.

Chain. Each node links to the node next in sequence and communication between the nodes is by passing information along the line. This organization is typical among networks that have a common function such as smuggling goods and people or laundering money.

Hub or Spoke and Wheel. Outer nodes communicate with one central node, which may not be the leader or decision maker for the network. A variation of the hub is a wheel design where the outer nodes communicate with one or two other outer nodes in addition to the hub. A wheel configuration is common for a financial or economic network.

All-Channel. All nodes are connected to each other. The network is organizationally “flat,” meaning there is no hierarchical command structure above it. Command and control (C2) is distributed within the network. This is communication intensive and can be a security problem if the linkages can be identified, reconstructed, and exploited. However, the lack of an identifiable “head” confounds the targeting and disrupting efforts normally effective against hierarchies.

As compared with a typical networked or hierarchical terrorist organization, the lone terrorist is often the hardest to detect, which presents a formidable challenge for law enforcement (LE) and intelligence agencies.

The **lone terrorist**’s tactics are conceived entirely on his own without any direction from a terrorist commander. Typically, the lone terrorist shares an ideological and sympathetic identification with an extremist organization and its goals, and may have had some limited level of direct affiliation in the past, but the lone terrorist does not communicate with any group as he fashions his political aims and commits acts of terrorism. Notably, it can be difficult to distinguish between a lone terrorist aiming for political results and another criminal, such as a serial killer, who uses the same tactics.

Identity and intent are linked closely to the underlying ideology and the corresponding strategic goals. Political or religious identity expressed in ideology is often all-encompassing and determines the general parameters — the “why” and “where” — of the terrorist operations.

Ideological categories describe the political, religious, or social orientation of the group.

Geographic designations are sometimes used to categorize terrorist groups, although they are often confusing. In some instances geography overlaps ethnic, national, and religious/ideological aspirations. In other

Some of the common **identity and intent** categories are:

Ethnocentric. Groups of this persuasion see race or ethnicity as the defining characteristic of a society, and therefore a basis of cohesion.

Nationalistic. Loyalty and devotion to a nation-state, and the national consciousness derived from placing one nation’s culture and interests above those of other nations or groups is the motivating factor behind these groups.

Revolutionary. These groups are dedicated to the overthrow of an established order and replacing it with a new political or social structure.

Separatist. Separatist groups are those with the goal of separation from existing entities through independence, political autonomy, or religious freedom or domination.

Political. Political ideologies are concerned with the structure and organization of the forms of government and communities. While observers outside terrorist organizations may stress differences in political ideology, the activities of groups that are diametrically opposed on the political spectrum are similar to each other in practice.

Religious. All of the major world religions have extremists that have taken up violence to further their perceived religious goals. Religiously motivated terrorists see their ultimate objectives as divinely sanctioned, and therefore infallible and nonnegotiable.

Social. Often particular social policies or issues will be so contentious that they will incite extremist behavior and terrorism. Frequently this is referred to as “single issue” or “special interest” terrorism.

Domestic or Indigenous. These terrorists are “home-grown” and typically operate within and against their home country. They are frequently tied to extreme political, religious, or social factions within a particular society and focus their efforts specifically on their nation’s sociopolitical arena.

International. Often describing the support and operational reach of a group, this term and transnational

instances it is less relevant when referring to international and transnational terrorism.

are often loosely defined, and can be applied to widely different capabilities. International groups typically operate in multiple countries, but retain a geographic focus for their activities.

Transnational. Transnational groups operate internationally, but are not tied to a particular country, or even region. Al-Qaeda is transnational, being made up of many nationalities, being based out of multiple countries simultaneously, and conducting operations throughout the world.

Joint doctrine identifies three types of state affiliations: non-state supported, state supported, and state directed terrorist groups.

Categorizing terrorist groups by their affiliation with states provides analysts indicators of their potential capabilities and targeting. Capabilities include the level and type of training, intelligence, logistic and operational support, funding, equipment, and weaponry. State affiliation may also be an indicator of probable targets and even preferred tactics, techniques, and procedures (TTP). A terrorist group's selection of targets and tactics is also a function of the group's affiliation, level of training, organization, and sophistication.

Typically, there are four different levels of commitment within a terrorist organization: passive supporters, active supporters, cadre, and leadership.

Leaders provide direction and policy, approve goals and objectives, and produce overarching guidance for operations.

Cadre are the zealots of a terrorist organization who not only plan and conduct operations, but also manage technology, intelligence, finance, logistics, information operations (IO), and communications. Mid-level cadres tend to be trainers and technicians such as bomb makers, financiers, and surveillance experts. **Low-level cadres are the bombers and direct action terrorists for other types of attacks.**

Active supporters participate in the political, fund-raising, and information activities of the group. Acting as an ally or tacit partner, they may also conduct initial intelligence and surveillance activities, and provide safe houses, financial contributions, medical assistance, and transit assistance for active cadre members in more of a logistical role. **Usually, they are fully aware of their relationship to the terrorist group but do not commit violent acts.**

Passive supporters are typically individuals or groups that are sympathetic to the announced goals and intentions of the terrorist organization, but are not committed enough to take action

Recruiting.

Terrorist groups recruit from populations that are sympathetic to their ideology and objectives. Often legitimate organizations can serve as recruiting grounds for terrorists. Some recruiting may be conducted on the basis of particular skills and qualifications, rather than ideological characteristics.

Terrorists employ a variety of tactics, techniques, and procedures—some small scale, some large scale—to produce fear in their intended audience.

Their targets may be just as likely economic (tourists, financial networks) or agricultural (livestock, crops), as they are embassies or military forces. Their goal is not just to win favor for their causes, but to erode the confidence, capability, and legitimacy of the government or societies they wish to coerce. The most common TTP employed by terrorist groups are: assassination, arson, bombing, kidnapping and hostage taking, hijacking, seizure, raids and ambushes, sabotage, threats and hoaxes, and environmental destruction.

The term terrorism is often used interchangeably with the term insurgency. What typically distinguishes terrorism is that while both terrorism and insurgency seek political aims, terrorism is always unlawful and specifically intended to inculcate fear to achieve its aims.

Terrorists prefer to attack their adversaries asymmetrically by circumventing an opponent's strength and exploiting his weaknesses.

Using this approach, terrorists pick the time, place, and manner of the attack while avoiding direct contact with their targets. Asymmetric tactics routinely employed by terrorist adversaries include:

Denial and Deception - Dispersion and hiding in complex terrain and urban environments degrade situational awareness and complicate US intelligence and targeting efforts

Human Shields - In their attacks, terrorists deliberately use civilians as human shields. This tactic forces friendly forces to adopt more stringent rules of engagement.

Ambush and Surprise Attacks - Terrorists avoid or desire to limit their direct fire engagements with heavy armored vehicles and prefer to conduct “standoff” attacks

with improvised explosive devices 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.

Information Operations. Terrorists have used IO to disrupt popular support for coalition forces and to garner regional and international sympathy and support for insurgent forces. Terrorists are adept at disseminating information quickly thus putting friendly IO in a defensive posture.

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 Nation. 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. 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.

Intelligence

Intelligence in AT. Accurate, timely, and relevant intelligence is critical in identifying and assessing terrorist capabilities, plans, intent, emerging trends, magnitude, probable courses of action, and possible targets. Each intelligence discipline contributes to AT capabilities through the use of signals intelligence, geospatial intelligence, measurement and signature intelligence, human intelligence, and open-source information. By integrating all available sources of intelligence, commanders have the basis for the development of an effective AT program. The ability of the intelligence enterprise to provide critical, relevant, and timely information to the user depends not only on efficient collection, processing, and exploitation, but also on the ability to organize, store, and rapidly retrieve, fuse, and disseminate this information.

Intelligence and risk management.

The AT program is a comprehensive effort focused on the detection and prevention of terrorist attacks against DOD personnel, their families, installations, and supporting infrastructure critical to mission accomplishment. Intelligence provides the commander with a threat analysis that reviews the factors of a terrorist group's operational capability, intentions, and activity, as well as the operating environment within which friendly forces operate. Commanders must carefully exercise judgment in estimating both the existing terrorist threat and the need for changes in AT measures.

Well-planned, proactive, systematic, all-source intelligence provides decision makers with information and timely warnings upon which to recommend force protection actions and build an effective AT program.

An effective AT program contributes to disruption of threat incidents through preventive measures and includes proactive and reactive phases. During the proactive phase, organizations perform threat and intelligence analysis, conduct information sharing, and compile criticality assessments (CAs) and vulnerability assessments (VAs) in order to develop a comprehensive threat assessment (TA). During the reactive phase, organizations perform crisis management actions and execute the commander's AT intent.

National-level AT intelligence roles and responsibilities.

Within the United States, the Federal Bureau of Investigation (FBI) is responsible for collecting and processing terrorist information to protect the US from terrorist attack. Overseas, terrorist intelligence is principally a Central Intelligence Agency (CIA) responsibility, but the Department of State (DOS), Defense Intelligence Agency (DIA), and host nation (HN) are also active players. Military intelligence activities are conducted in accordance with presidential executive orders, federal law, status-of forces agreements (SOFAs), memorandums of understanding (MOUs), and applicable Service regulations.

DOD-level AT intelligence roles and responsibilities.

DIA. The Director, DIA, under the Under Secretary of Defense for Intelligence, is responsible for establishing and maintaining an international all-source terrorism intelligence fusion center, Joint Intelligence Task Force-Combating Terrorism (JITF-CT). The JITF-CT provides a wide range of terrorism intelligence for DOD components, to include indications and warnings, current intelligence, assessments, in-depth analysis, DOD terrorism threat assessments/levels, and the maintenance of a combating terrorism database.

GCCs. The GCC, through the intelligence directorate of a joint staff, joint intelligence operations center, command counterintelligence coordinating authority, and subordinate component commands' CI and AT organizations, and in consultation with DIA, CIA, US country team, and applicable HN authorities, compiles intelligence and CI information specific to the operational area and issues intelligence and CI reports, advisories, and assessments.

Services. 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, law enforcement (LE), and CI organizations with national level intelligence, surveillance, and reconnaissance collection activities.

Investigative Agencies. Service criminal investigative services (e.g., United States Army Criminal Investigation Command, Naval Criminal Investigative Service, Air Force Office of Special Investigations) 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.

Information Requirements. To focus threat analysis, the intelligence staff identifies significant gaps in what is known about the adversary and other relevant aspects of the operational environment and formulates intelligence requirements (general or specific subjects upon which there is a need for the collection of information or the production of intelligence).

Legal Considerations

Commanders have both the inherent authority and the responsibility to enforce security measures and to protect persons and property under their control. Commanders

should consult with their legal advisors regularly when establishing their AT programs.

DOD is the lead agency for conducting overseas HD operations. However, against internal threats (e.g., domestic terrorism), DOD may be in support of Department of Justice or Department of Homeland Security and may conduct civil support operations for declared emergencies.

Commanders' responsibilities inside the United States and its territories and possessions.

Although the FBI has primary LE responsibility for investigating terrorist incidents inside the US (including its possessions and territories) and the DOD LE and intelligence community have a significant role within their departmental areas of jurisdiction, commanders remain responsible for maintaining law and order on DOD installations and vessels.

Commander's responsibilities outside the United States and its territories and possessions.

Although DOS has the primary responsibility for dealing with terrorism involving Americans abroad, DOD commanders have the inherent right 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 GCC for further reporting to DOS. The commander is responsible for incident response and containment in order to protect DOD personnel and property from immediate threat of injury. DOS has the primary responsibility for coordinating the political and diplomatic response to terrorism involving Americans abroad.

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.

Memorandum of understanding and memorandum of agreement.

Title 22, United States Code, Section 4802, directs the Secretary of State (SECSTATE) to assume responsibility for the security of all US Government (USG) personnel on official duty abroad, except those under the command of GCCs 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—GCC or COM—in the most efficient and effective position to provide security for DOD elements and personnel. The MOU requires delineation of security responsibilities through country-specific MOAs.

Antiterrorism Program

The minimum elements of an AT program are AT risk management, planning, training and exercises, resource management, and a program review.

Protection of DOD personnel and assets from acts of terrorism is one of the most complex challenges for commanders. AT programs consist of defensive measures to reduce the vulnerability of individuals and property to terrorist acts, including rapid containment by local military and civilian forces. An integrated and comprehensive AT program (physical security, construction standards, CBRN passive defense, OPSEC, CI, biometrics and forensics exploitation, etc.) must be developed, implemented, and updated in order to effectively detect, defend, and respond to a terrorist threat.

Risk management process.

The risk management process is used in identifying, assessing, and mitigating risk arising from operational factors and making decisions that balance risk and cost with mission benefits. AT risk management allows the commander to decide how best to employ given resources and AT measures to deter, prevent, or mitigate a terrorist attack, balancing risk and cost while ensuring mission readiness

AT planning.

AT planning is the process of developing specific guidance, measures, and instructions to deter, mitigate, and prepare for a terrorist incident. The AT plan contains command-specific guidance to establish and maintain an AT program as outlined in DODI 2000.16, *DOD Antiterrorism (AT) Standards*. At a minimum, AT plans shall be developed at the installation, separate or leased facility or space, and ship levels, and also for operational deployments, training exercises or events, and special events.

AT training and exercises.

An AT program must include training for development of individual, leader, and collective skills, and the conduct of comprehensive exercises to validate AT plans.

Program review.

A program review is required at least annually, during predeployment preparations and when significant changes occur regarding threat, asset criticality, or vulnerability.

Antiterrorism plan development.

AT plans should prepare for the most likely threats and should maximize the use of existing plans and standing operating procedures (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.

At a minimum, an AT plan must include measures that take into account the key elements of the AT program.

AT measures should include random antiterrorism measures, provisions for the use of physical structures, physical security equipment, CBRN detection and protection equipment, response forces, and other emergency response measures. All AT measures should be **scalable** and **proportional** to increases in the local threat and/or unit operational capability.

Risk management process.

TA, CA, and VA are used to produce an over-all risk assessment. Use the final risk assessment as a guide to risk mitigation priorities and establish a local baseline or defense posture.

Physical security.

Physical security measures incorporate facilities, equipment, trained personnel, and procedures into a comprehensive effort designed to provide optimal AT protection to personnel and assets. AT plans should include notifications to the appropriate emergency responders, including LE offices, and the servicing FBI field office enabling 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.

Incident response.

Terrorist incident response ensures C2 communications and intelligence are provided to emergency responders charged with determining the full nature and scope of the incident, mitigating the damage, and countering any remaining terrorist(s).

Training and exercises.

AT plans are exercised annually and whenever possible should be conducted in coordination with federal, local,

	state, tribal, or HN authorities and US embassies and consulates.
<i>AT resource management.</i>	AT resource requirements can be identified via DOD's Planning, Programming, Budgeting, and Execution process, as well as available supplemental programs such as Combatant Commander's Initiative Fund.
<i>Program review.</i>	The program review evaluates the effectiveness and adequacy of the commander's AT program.
<i>Countering terrorist attack planning.</i>	Effective AT programs aim to detect, disrupt, and potentially defeat terrorist attack planning in order to ensure the safety of personnel and resources. To achieve this, AT plans should examine terrorist methods of surveillance, information gathering, and attack planning to determine the extent of training and resources needed to address the threat. In addition, AT plans must identify the most effective way to train personnel to counter terrorist attack planning with basic surveillance awareness procedures. Most important, AT programs need to focus on building strong relationships with various LE and CI agencies. Indeed, this is a critical step in increasing the flow of information to neutralize the threat.
<i>Terrorist methods of surveillance and information gathering.</i>	Effective AT programs aim to prevent or disrupt attacks by focusing on the initial stages in the terrorist attack planning process, where terrorists conduct initial surveillance and select targets for exploitation and suitability for attack. Five techniques in the methodology that contributes to the terrorist attack planning cycle are fixed (static) surveillance, mobile surveillance, technical surveillance, casual questioning (elicitation), and probing.
<i>Surveillance awareness.</i>	DOD personnel and their families must understand the implications of hostile surveillance; to assume that it is occurring, how to discretely detect or identify it, and what to do if they suspect it. In fact, personnel are often able to detect criminal or terrorist surveillance (i.e., targeting themselves or their installations) as a result of enhanced situational awareness orchestrated by aggressive AT programs. They may even make themselves less desirable targets by following the four fundamental principles of surveillance awareness: stay informed, keep a low profile, be unpredictable, and stay alert.

Surveillance detection.

Surveillance detection operations take it a step further by providing a commander the ability to move beyond ordinary FP measures and incident response to operations that will directly deter, detect, disrupt, and ultimately defeat the terrorist attack planning cycle. Simply stated, surveillance detection operations are used to detect and/or verify whether an individual, vehicle, or location is under surveillance.

Counterintelligence and LE resources.

Regardless of the AT capabilities, resources, and protective measures in place, close working relationships with local, state, HN, and federal LE agencies are essential to establishing timely and effective responses to 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 the overall security of their units and the military community at large.

Incident reporting.

Since terrorists frequently conduct extensive target surveillance—over a period of weeks, months, or years—their activities should be detectable. Moreover, terrorists will invariably commit mistakes, further increasing the chance of detection by ordinary individuals, security personnel, and trained surveillance detection teams. AT plans therefore require the most streamlined processes to expedite incident reporting of unusual activities so that information moves rapidly from the originator, through security and military police, and over to the required investigative and CI organizations. The best incident reports include detailed descriptions of the subject(s), time of day, locations, vehicles involved, and the circumstances of the sightings. Military police and security personnel need to report these incidents to their respective criminal investigative services or CI elements as soon as possible.

Terrorist Incident Response

An important objective of AT incident response is to mitigate the number and severity of casualties resulting from a terrorist attack.

The response to a terrorist incident includes procedures established to mitigate the effects of the incident. These procedures are designed to ensure the commander is able to rapidly deploy a terrorist incident response team to reduce further effects and damage; support emergency lifesaving and rescue functions; provide protection of

DOD personnel and property; and, when appropriate, conduct or support criminal investigations. Well developed response measures can save lives, preserve health and safety, protect and secure property, and eliminate the hazard. A slow or uncoordinated response may result in additional loss of life, further damage to the installation, and the loss of public confidence in the organization's ability to respond to a terrorist incident.

It is incumbent upon the commander to plan for, and be capable of reacting to, a terrorist attack using available assets until outside assistance arrives.

Terrorist incident response measures should include procedures for determining the nature and scope of incident response and procedures for coordinating security, fire, HAZMAT, and medical emergency responders. Although not direct elements of AT, plans for managing the consequences of a CBRN incident and continuity of essential military operations are important adjuncts to an effective AT program.

At a minimum, AT plans should prepare for the most probable or likely threats as identified through the TA process and maximize the use of existing plans and SOPs. 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 comprise the emergency operations center (EOC) during an actual crisis.

The onset of a terrorist incident begins with the detection of an unlawful act of violence or the threat of violence.

Detection may result from routine surveillance performed by an installation or facility intrusion-detection system, guard or security force, or in the case of bioterrorism, an unusual incidence of an infectious disease. Once detection of a terrorist act or incident has occurred, an initial assessment must be conducted by the first responding LE or security detachment.

Responses will vary according to the incident.

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 and all installations/ships must have trained personnel who are aware of the threat and are capable of reacting promptly 24 hours a day.

Emergency operations center.

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. 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.

Confirmation.

Since the categorization of an incident will be a relevant factor in determining jurisdiction, 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.

Initial response to a chemical, biological, radiological, or nuclear attack.

Installations are required to establish an immediate response capability to ensure critical mission continuity and save lives during a CBRN incident and to mitigate the situation. 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.

Special considerations.

A crucial aspect of implementing the AT plan is establishing communications among the forces in the incident area and the EOC. Communications personnel must be able to respond to changing needs during the incident and be able to maintain communications channels.

Although the primary goal is ending a terrorist incident without injury, another goal is the successful prosecution of terrorists. Witness testimony, photographic evidence, and other evidence, are important in achieving a successful prosecution.

Principal public affairs 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.

Considerations in the United States / National Incident Management System (NIMS).

The National Response Framework (NRF) specifies how the resources of the USG will work in concert with state, local, and tribal governments and the private sector to respond to incidents of national significance. The NRF is predicated on National Incident Management System (NIMS) and together, they provide a nationwide template for working together to prevent or respond to threats and incidents regardless of cause, size, or complexity. NIMS is a comprehensive national approach to incident management that is applicable at all jurisdictional levels and across functional disciplines.

NIMS standard incident management structures are based on four key organizational systems.

The **incident command system**, which defines the operating characteristics, management components, and structure of incident management organizations throughout the life cycle of an incident.

Multiagency coordination systems, which define the operating characteristics, management components, and organizational structures of supporting entities.

Civil authority information support is an authorized DOD capability for communicating information to domestic populations during national emergencies, such as terrorist incidents or natural disasters.

Public information systems, which include the processes, procedures, and systems for communicating timely and accurate information to the public during emergency situations.

CONCLUSION

This publication provides joint doctrine for planning, executing, and assessing joint antiterrorism operations.

Intentionally Blank

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

a. Terrorists pose a grave danger to the national security and interests of the United States at home and abroad. The National Strategy for Combating Terrorism outlines a strategic vision built around an international effort aimed at the defeat of violent extremism which threatens the way of life for free and open societies and creation of a global environment inhospitable to violent extremists and their supporters. Additionally, some traditional criminal activities, such as counterfeiting or illegal drug trafficking, may be terrorist related if used to fund terrorist acts. Although there is no universal definition for terrorism, the Department of Defense (DOD) defines it as **the unlawful use of violence or threat of violence to instill fear and coerce governments or societies. Terrorism is often motivated by religious, political, or other ideological beliefs and committed in the pursuit of goals that are usually political.**

b. **Combating Terrorism (CbT).** The broader construct of CbT is defined as actions, including antiterrorism and counterterrorism, taken to oppose terrorism throughout the entire threat spectrum. Historically, CbT has been both a battle of arms and ideas—a fight against the terrorists and the ideology which drives terrorism. CbT remains an approach with both defensive and offensive components: antiterrorism (AT)—defined as **defensive measures used to reduce the vulnerability of individuals and property to terrorists acts, to include rapid containment by local military and civilian forces;** and counterterrorism (CT)—defined as **actions taken directly against terrorists networks and indirectly to influence and render global and regional environments inhospitable to terrorist networks.** Critical supporting functions of CbT are intelligence support, information sharing, and incident management, which together serve to support and link AT and CT in the achievement of common strategic objectives (see Figure I-1). Other defensive elements that also overlap in large part with CbT are force protection (FP), personal security, operations security (OPSEC), continuity of operations (COOP), counter weapons of mass destruction (WMD), and Defense Critical Infrastructure Program (DCIP) efforts.

c. This publication does not expand upon CT. For more information on CbT and CT, see Joint Publication (JP) 3-26, *Counterterrorism*. Specific policy, directive guidance, standards, and procedures for the DOD AT program are contained in DOD Directive

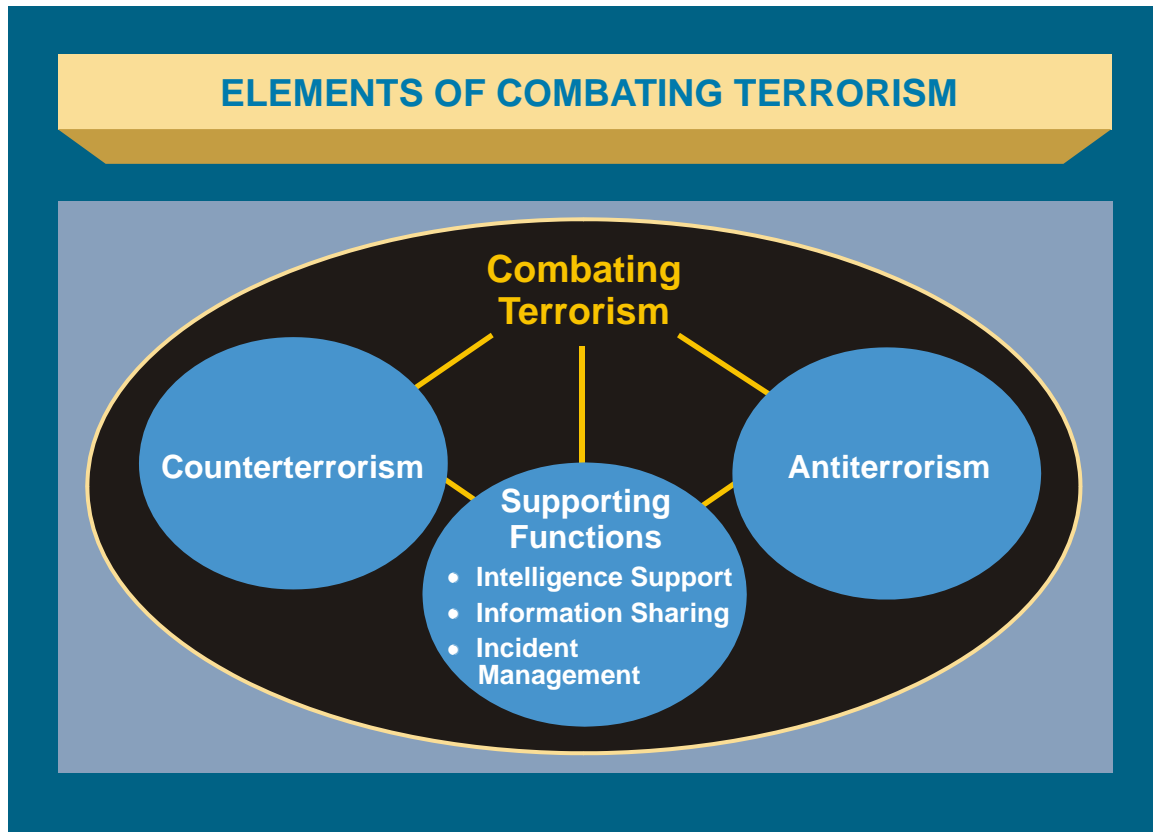


Figure I-1. Elements of Combating Terrorism

(DODD) 2000.12, *DOD Antiterrorism (AT) Program*, and Department of Defense Instruction (DODI) 2000.16, *DOD Antiterrorism (AT) Standards*.

2. Antiterrorism in the Context of Other Protection Efforts

a. AT is one of several requirements under a commander's overall responsibility to provide protection. Indeed, commanders use a breadth of complementary programs to protect designated personnel, assets, processes, information, and interdependent networks and systems from a variety of threats including terrorism. Certain programs focus on **active defense measures** that protect the joint force, its information, its bases, necessary infrastructure, and lines of communications from an adversary's attack. Some involve **passive measures** (e.g., concealment or OPSEC) that make friendly forces, systems, and facilities difficult to locate and destroy. Other programs apply **technology and procedures** (e.g., biometrics) to reduce risk, while some focus on **incident response** and emergency preparedness to reduce the loss of personnel and capabilities due to accidents, health threats, and natural disasters.

b. As required or directed, the protection of forces, including the use of AT programs, may be extended to encompass protection of US noncombatants; the forces, systems, and civil infrastructure of friendly nations; and other government agencies, intergovernmental organizations, and nongovernmental organizations (NGOs).

c. Certain protection efforts, such as FP; COOP; critical infrastructure protection (CIP); information assurance; chemical, biological, radiological, and nuclear (CBRN) defense; readiness; and installation preparedness, are inherently connected to AT, though these programs may also focus on, for example, criminal and conventional threats.

d. **Force Protection and Antiterrorism.** AT is not only a sub-element of CbT, but it is also a subset of the broader FP construct (see Figure I-2). FP is defined as **preventive measures to mitigate hostile actions against DOD personnel (to include family members), resources, facilities, and critical information. FP does not include actions to defeat the enemy or protect against accidents, weather, or disease.** While AT programs also integrate various FP-related programs to protect against terrorist attacks (physical security, CBRN passive defense, OPSEC, counterintelligence [CI], biometrics, and surveillance detection, etc.), it does not include all aspects of FP. That said, plans and capabilities developed for AT should be coordinated with other crisis management efforts in order to prevent or minimize redundant programs.

For information on WMD active defense, CBRN passive defense, and the relationship between CbT and combating WMD, see JP 3-40, Combating Weapons of Mass Destruction, and JP 3-11, Operations in Chemical, Biological, Radiological, and Nuclear (CBRN) Environments.

3. Overview of Antiterrorism Program

a. 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 associated infrastructure critical to mission accomplishment as well as the preparations to defend against and plan for the response to the consequences of terrorist incidents. The minimum elements of an AT program are: risk management (RM); planning; training and exercises; resource management; public awareness; and comprehensive program review. AT program elements should be iterative and serve to continuously refine the AT plan. Commanders should also develop working relationships with interagency partners as necessary to ensure the comprehensive and coordinated implementation of AT plans.

For more information, see Chapter V, “Antiterrorism Programs,” and Appendix E, “Risk Management Process.”

b. **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. 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. The risk management process consists of three key elements—**threat, criticality, and vulnerability**—which are used to produce a final **risk assessment (RA)**.

4. Overview of Department of Defense Roles and Responsibilities

a. DOD Policy

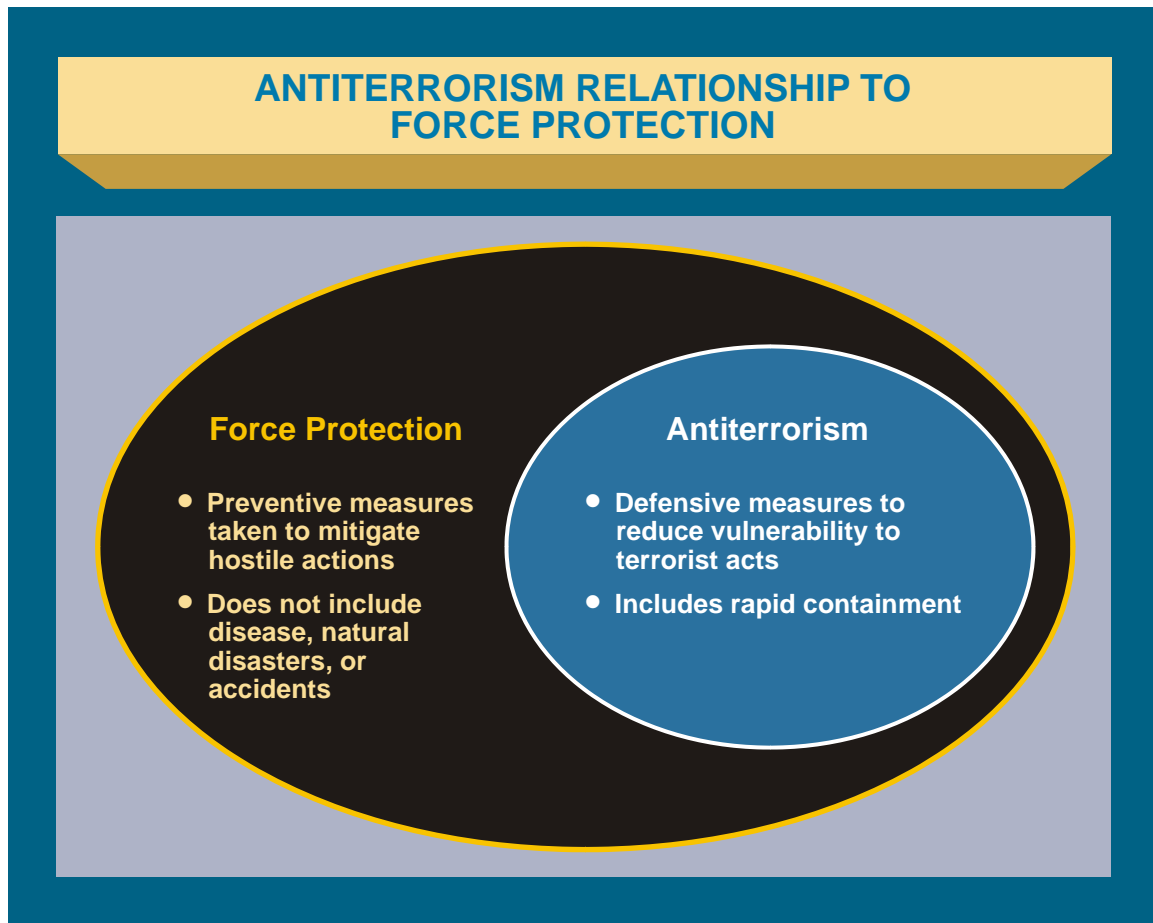


Figure I-2. Antiterrorism Relationship to Force Protection

(1) The DOD components, elements, and personnel shall be protected from terrorist acts through a high priority, comprehensive AT program 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 subject to their control, including deployed DOD contractors authorized to accompany the force and other contractor personnel requiring access to military facilities, as referenced in DODI 3020.41, *Contractor Personnel Authorized to Accompany the US Armed Forces*. Commanders should ensure the AT awareness and readiness of all DOD elements and personnel (including dependent family members) assigned or attached.

(3) The geographic combatant commanders' (GCCs') AT policies take precedence over all AT policies or programs of any DOD component operating or existing in that GCC's area of responsibility (AOR) except for those under the security responsibility of a chief of mission (COM). All DOD personnel traveling into or through a GCC's AOR will familiarize themselves with all AOR and country-specific AT policies and comply with them.

(4) A funding source for emergent or emergency AT requirements is the Combatant Commander Initiative Fund (CCIF). For more information, refer to Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 7401.01D, *Combatant Commander Initiative Fund*.

(5) All personnel on DOD-related travel shall comply with theater, country, and special clearance requirements (DOD 4500.54E, *DOD Foreign Clearance Program [FCP]*), 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) **Contractors.** Protection of contractors is a shared responsibility between the contractor and the government.

For further information on FP and security of contractors, see DODI 3020.41, Contractor Personnel Authorized to Accompany the US Armed Forces, and JP 4-10, Operational Contract Support.

(7) Compliance with the “no double standard” policy on dissemination of terrorist threat information is maintained. (See Chapter III, “Intelligence.”)

b. DOD Responsibilities

(1) **Assistant Secretary of Defense for Homeland Defense and Americas’ Security Affairs (ASD[HD&ASA]).** The ASD(HD&ASA) provides overall supervision of AT, homeland defense (HD), DCIP, and civil support activities within DOD. Specific to AT, the ASD(HD&ASA) has the following responsibilities:

(a) Oversee high-risk personnel (HRP) program.

For more information on HRP, refer to DODI O-2000.22, Designation and Physical Protection of DOD High Risk Personnel (HRP).

(b) Serve as Antiterrorism Coordinating Committee—Senior Steering Group Co-Chair.

(c) 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.

(d) Provide policy and guidance for DCIP and oversee implementation of the program.

(2) **The Secretaries of the Military Departments have the following responsibilities:**

(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 (AT) Standards*. Ensure personnel traveling to a GCC's AOR comply with DODD 4500.54E, *DOD Foreign Clearance Program (FCP)*. Ensure personnel are aware of any Department of State (DOS) travel warnings and alerts in effect at the time of travel.

(3) The Chairman of the Joint Chiefs of Staff has the following responsibilities:

(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(HD&ASA) 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 AT training for all DOD personnel (including their dependent family members) in conjunction with DOD components.

(c) Assist ASD(HD&ASA) with centralized policy and standard development for HRP programs, training, and support.

(d) 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.

(e) Assess AT as an element of the overall force planning function of any force deployment decision. Periodically reassess CCDR's AT posture of deployed forces.

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

(g) Provide representatives to the DOD ATCC and appropriate subcommittees, as well as an observer to the Overseas Security Policy Board.

(h) Coordinate with the Under Secretary of Defense for Intelligence and the ASD(HD&ASA) on sharing of terrorism intelligence and CI data and information on AT.

(i) 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 suspicious activity reports (SARs) from military security, law enforcement (LE), and CI organizations with national-level intelligence, surveillance, and reconnaissance (ISR) collection activities.

(j) Manage and administer CJCS CCIF.

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

(l) Maintain the Antiterrorism Enterprise Portal (ATEP) (see Figure I-3).

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

(4) GCCs have overall AT responsibility within their AOR, except for those DOD elements and personnel for whom a COM has security responsibility pursuant to law or a memorandum of agreement (MOA). Accordingly, GCCs have the following responsibilities:

(a) Establish AT policies and programs for the protection of all DOD elements not under the authority of COM within their AOR.

(b) Ensure AT policies and programs include specific prescriptive standards derived from DODI 2000.16, *DOD Antiterrorism (AT) Standards*, to address specific terrorist capabilities and geographic settings, particularly regarding defense of critical infrastructure necessary for mission accomplishment (as defined in DODD 3020.40, *Defense Critical Infrastructure Program [DCIP]*), and other DOD-owned, leased, or managed mission essential assets.

(c) Exercise tactical control (TACON) for FP over all DOD elements and personnel (including DOD dependents, except those under the security responsibility of a COM) within the GCC's AOR. TACON (for FP) applies to all DOD personnel assigned, permanently or temporarily, transiting through, or performing exercises or training in the GCC's AOR. TACON (for FP) is in addition to a GCC's normal exercise of operational control over assigned forces.

(d) 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, except for elements and personnel for whom the COM accepts or retains security responsibility (see Chapter IV, "Legal Considerations"). 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

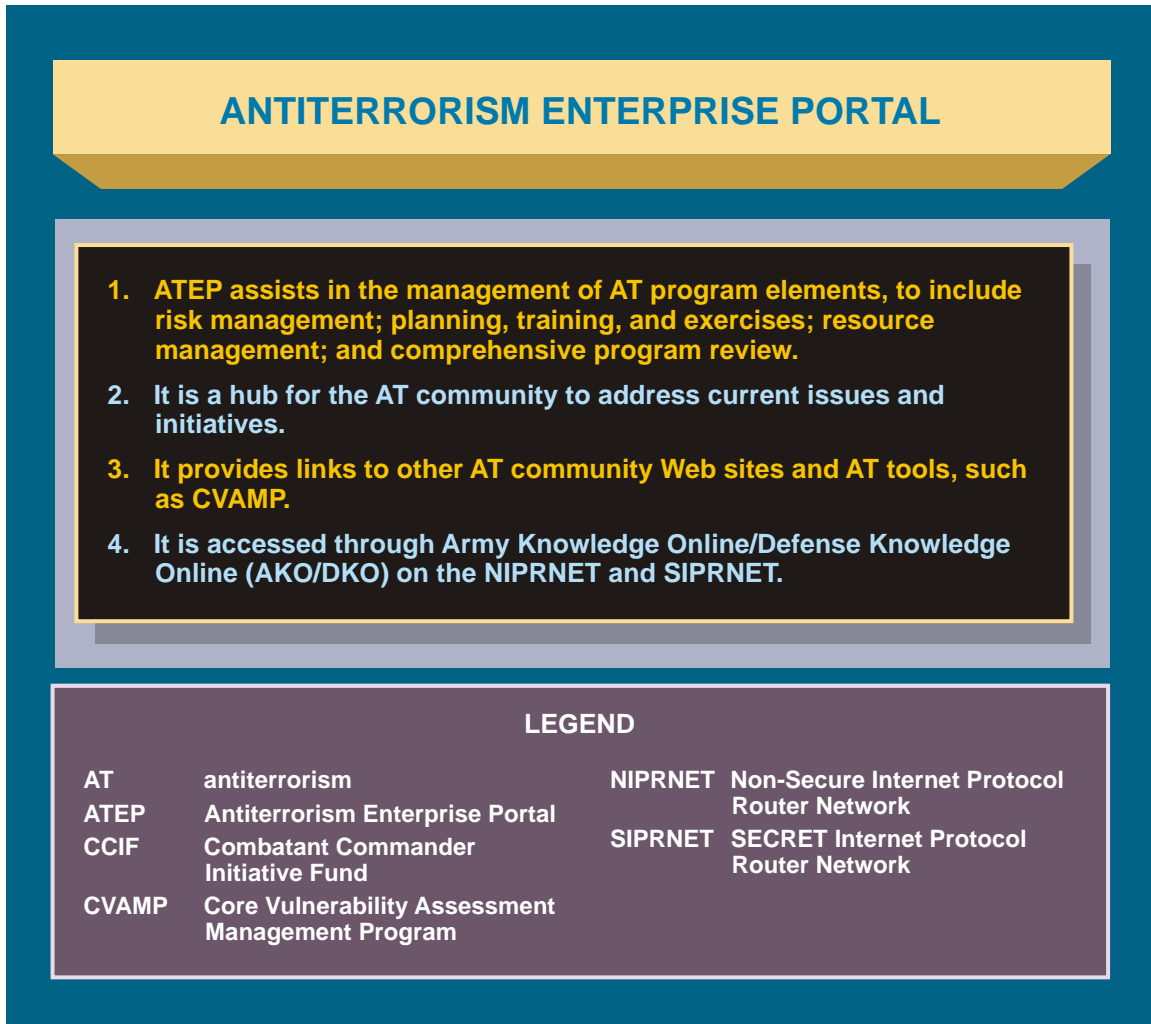


Figure I-3. Antiterrorism Enterprise Portal

asset criticality, terrorist threat, and vulnerabilities. AT program reviews shall also evaluate installation and activity preparedness to respond to terrorist incidents (including CBRN incidents), and the plans for responding to terrorist incidents and maintaining continuity of essential military operations. Relocate forces as necessary and report to SecDef through CJCS pertinent actions taken for protection.

(e) Consistent with DODI 5210.84, *Security of DOD Personnel at US Missions Abroad*, DODI 5240.22, *Counterintelligence Support to Force Protection*, and all appropriate memorandums of understanding (MOUs), serve as the DOD point of contact with host nation (HN) officials on matters involving AT policies and programs.

(f) Provide updates to DODD 4500.54E, *DOD Foreign Clearance Program (FCP)*, stating command travel requirements and theater entry requirements.

(g) Upon arrival in their AOR, 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 (AT) Standards*. Ensure personnel traveling

within or through their AOR comply with DODD 4500.54E, *DOD Foreign Clearance Program (FCP)*. Ensure personnel are aware of any DOS travel warnings and alerts 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 receive required AT training and briefings (e.g., AOR updates) in compliance with DODI 2000.16, *DOD Antiterrorism (AT) Standards*, before departing their previous assignment. Identify and disseminate to deploying force providers specific AOR predeployment training requirements that all personnel, including contractors authorized to accompany the force, must complete before arrival in theater. All contingency contractor personnel shall comply with applicable GCC and local commander FP policies.

(h) 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 GCC 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.

(i) 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.

(j) 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.

(k) 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.

(l) Ensure compliance with the “no double standard” policy (see Chapter III, “Intelligence”).

(m) Submit to CJCS emergent or emergency AT fund requests as required.

(n) Ensure FPCONs are implemented and disseminated.

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

(p) Provide a representative to the DOD ATCC and appropriate subcommittees, as required in DODD 2000.12, *DOD Antiterrorism (AT) Program*.

(q) 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 biometrics enabled intelligence and suspicious activity reports from military security, LE, and CI organizations with national-level ISR collection activities.

(r) Ensure that subordinate commanders establish screening and access control policies and procedures for all personnel, to include contractor employees, requiring access to DOD installations consistent with DOD 5200.08 and 5200.08-R. This requirement is especially pertinent to contractors who have not been issued common access cards.

(5) Functional combatant commanders have the following responsibilities:

(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 GCC and, in coordination with the GCC, the COM.

(b) Coordinate with the GCCs to ensure adequate AT measures are in place.

(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 CCDR and the Service component command chain of command.

(d) Submit emergent or emergency AT fund requests to CJCS.

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

(f) 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.

(g) Develop their own CCDR-oriented AT strategic plan that details the vision, mission, goals, and performance measures in support of the DOD and GCCs' AT strategic plans.

(6) Directors of other DOD agencies and components have the following responsibilities:

(a) Support GCCs as they execute their AT programs. Institute AT programs of their own which include vulnerability assessments and contingency response plans.

(b) Utilize DODI 2000.16, *DOD Antiterrorism (AT) 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 CCDR to ensure AT policies and programs are in concert with the GCCs' overall responsibility for the AOR.

(c) Comply with DODI 2000.16, *DOD Antiterrorism (AT) Standards*, requirements to maintain an AT training and exercise program. Ensure that all assigned personnel comply with DODD 4500.54E, *DOD Foreign Clearance Program (FCP)*. 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, *DOD Antiterrorism (AT) Standards* before departing their current assignment.

(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 process, identify and document resource requirements necessary to implement and maintain AT programs. Submit AT requirements to SecDef with an information copy to CJCS and the appropriate combatant commanders. Include resource requirements in program and budget submissions. For emergent or emergency AT requirements that cannot be funded through other means, submit requests through the appropriate CCDR to CJCS. 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] UFC 4-020-01; *DOD Security Engineering Facilities Planning Manual*; UFC 4-010-01, *DOD Minimum Antiterrorism Standards for Buildings*; UFC 4-022-01, *Security Engineering: Entry Control Facilities/Access Control Points*; 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. **Agency Leads.** With respect to CT and other HD concerns, DOD is not the lead agency, but has significant supporting roles in several areas. In HD 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.”

For more information on operations in the homeland, see JP 3-27, Homeland Defense, and JP 3-28, Civil Support.

CHAPTER II

TERRORIST THREAT

“Terrorism is an arm the revolutionary can never relinquish.”

Carlos Marighella
Minimanual of the Urban Guerrilla

1. Threat of Terrorism

This chapter provides a general overview of terrorism. The current terrorist paradigm involves a broad spectrum of threats including traditional state-sponsored terrorism, networks of non-state actors, extremist groups, criminal networks, and radicalized individuals acting alone. A critical factor in understanding terrorism is the importance of the emotional and psychological impact of terrorism. Terrorists use violence or the threat of violence to impact multiple audiences. A clear understanding of the enemy remains fundamental to ensuring the safety of US citizens at home and abroad from the threat of terrorism.

2. Terrorist Organizational Structures

A general knowledge of prevalent terrorist organizational structures helps to understand their capabilities and the type of threat they pose. A terrorist organization's structure, along with membership, resources, and security determine in part its capabilities, influence, and reach. Terrorist groups, regardless of ideology, location, or structure, have some common basic organizational imperatives: the need to survive and to pursue the goals of the organization, while remaining credible to their followers.

a. **Basic Organizational Structure.** There are two typical organizational structures used by terrorist groups: **hierarchical and networked**. Newer groups tend to organize or adapt to the networked model, while others associated with political organizations prefer the more centralized control of the hierarchical structure to coordinate violent action with political action. Most groups are composed of both structures, continuously adapting as the strategic environment dictates. Within either of those two larger organizational structures, however, virtually all terrorist groups organize as smaller cells at the tactical level.

(1) **Hierarchical Structure.** These organizations have a well-defined vertical chain of command and responsibility. Information flows up and down organizational channels that correspond to these vertical chains, but may not move horizontally through the organization. Hierarchies are traditional and common of larger groups that are well established with a command and support structure. Hierarchical organizations feature greater specialization of functions in their subordinate cells (support, operations, intelligence). In the past, some significant “traditional” terrorist organizations influenced by revolutionary theory or Marxist-Leninist ideology used this structure: the Japanese Red Army, the Red Army Faction in Germany, the Red Brigades in Italy, the Palestine Liberation Organization, the Provisional Irish Republican Army (IRA), the Weather Underground, the

Symbionese Liberation Army, and the New World Liberation Front. These organizations had a clearly defined set of political, social, or economic objectives, and tailored aspects of their organizations (such as a “political” wing or “social welfare” group) to facilitate their success. The necessity to coordinate actions between various “fronts,” some political and allegedly nonviolent, and the use of violence by terrorists and some insurgents, favored a strong hierarchical structure. The benefits of hierarchies include greater efficiency due to specialization and ability to coordinate actions toward a common goal.

(2) **Networked Structure.** Unlike hierarchies, networks distribute authority and responsibility throughout an organization, often creating redundant key functions. To be effective, networks require a unifying idea, concern, goal, or ideology. Without a unifier, networks may take actions that are counterproductive, and independent nodes may not develop the necessary cohesiveness for success of the network. General goals and targets are announced, and individuals or cells with redundant capabilities are expected to use flexibility and initiative to conduct the necessary actions.

(a) Networks with cell structures allow anonymity of individuals operating throughout the organizational spectrum. Only the cell leader has knowledge of other cells or contacts, and only senior leadership has visibility of the entire organization. The various cells do not need to contact other cells, except for cells essential to a particular operation with which they are working in common. The avoidance of unnecessary coordination or command approval for action provides deniability to the leadership and enhances operations security. Furthermore, breaches in security do not paralyze or cripple the entire organization.

(b) Terrorist groups are now increasingly part of a far broader but indistinct system of networks than previously experienced. Rapid changes in leadership, whether through generational transition, internal conflict, or as a response to enhanced security operations, may signal significant adjustments to terrorist group organizational priorities and its capabilities. A network structure may be a variation of several basic nodal concepts, a node being an individual, a cell, another networked organization, or even a hierarchical organization. A terrorist network may consist of parts of other organizations (even governments), which are acting in ways that can be exploited to achieve the network’s organizational goals. Networks need not be dependent on the latest information technology to be effective. The organizational structure and the flow of information inside the organization (i.e., their information management plan) are the defining aspects of networks. While information technology can make networks more effective, low technology means such as couriers also enable networks to operate effectively.

b. **Basic Types of Networks.** There are three basic types of network structures, depending on the ways in which elements (nodes) are linked to other elements of the structure: the chain, hub (or spoke and wheel), and all-channel. A terrorist group may also employ a structure that combines elements of more than one network type. For example, a transnational terrorist organization might use chain networks for its money-laundering activities, tied to a hub network handling financial matters, tied, in turn, to an all-channel leadership network to direct the use of the funds into the operational activities of a hub network conducting pre-targeting surveillance and reconnaissance. An organizational structure that may appear very complex during the initial assessments of terrorist groups may

be more understandable when viewed in the context of chain, hub, or all channel networks variants or a combination of these structures.

(1) **Chain.** Each node links to the node next in sequence and communication between the nodes is by passing information along the line. This organization is typical among networks that have a common function such as smuggling goods and people or laundering money.

(2) **Hub or Spoke and Wheel.** Outer nodes communicate with one central node, which may not be the leader or decision maker for the network. A variation of the hub is a wheel design where the outer nodes communicate with one or two other outer nodes in addition to the hub. A wheel configuration is common for a financial or economic network.

(3) **All-Channel.** All nodes are connected to each other. The network is organizationally “flat,” meaning there is no hierarchical command structure above it. Command and control (C2) is distributed within the network. This is communication intensive and can be a security problem if the linkages can be identified, reconstructed, and exploited. However, the lack of an identifiable “head” confounds the targeting and disrupting efforts normally effective against hierarchies.

3. Lone Terrorist

As compared with a typical networked or hierarchical terrorist organization, the lone terrorist is often the hardest to detect, which presents a formidable challenge for LE and intelligence agencies. The lone terrorist’s tactics are conceived entirely on his own without any direction from a terrorist commander. Typically, the lone terrorist shares an ideological and sympathetic identification with an extremist organization and its goals, and may have had some limited level of direct affiliation in the past, but the lone terrorist does not communicate with any group as he fashions his political aims and commits acts of terrorism. Notably, it can be difficult to distinguish between a lone terrorist aiming for political results and another criminal, such as a serial killer, who uses the same tactics.

4. Identity Based Terrorism

a. **Identity and Intent Categories.** Identity and intent are linked closely to the underlying ideology and the corresponding strategic goals. Political or religious identity expressed in ideology is often all-encompassing and determines the general parameters — the “why” and “where” — of the terrorist operations. These factors determine the desired end state and measures of success for terrorists. Operational tactics, techniques, and procedures (TTP), specific targets, and timing are often constrained or limited by ideological frameworks — this may not be the case for some apocalyptic religious ideologies or political constructs. To make matters even more difficult many categories overlap, even when there would seem to be inherent ideological conflict. Some of the common categories are:

(1) **Ethnocentric.** Groups of this persuasion see race or ethnicity as the defining characteristic of a society, and therefore a basis of cohesion. These groups often desire their

full sovereignty making ethno-national terrorist groups among the most prevalent type of terrorist organization.

(2) **Nationalistic.** Loyalty and devotion to a nation-state, and the national consciousness derived from placing one nation's culture and interests above those of other nations or groups is the motivating factor behind these groups. This can find expression in national minorities living in other states.

(3) **Revolutionary.** These groups are dedicated to the overthrow of an established order and replacing it with a new political or social structure. Most terrorist groups are opposed to the established order and use terrorism as a revolutionary tactic to achieve their goals. Some state directed terrorist groups may use terrorism as a means to preserve and extend their power and/or as a strategic deterrent.

(4) **Separatist.** Separatist groups are those with the goal of separation from existing entities through independence, political autonomy, or religious freedom or domination. The ideologies separatists subscribe to include social justice or equity, anti-imperialism, as well as the resistance to conquest or occupation by a foreign power.

b. **Ideological Categories.** Ideological categories describe the political, religious, or social orientation of the group. While some groups will be seriously committed to their avowed ideologies, for others, ideology is poorly understood, and primarily a rationale used to provide justification for their actions to outsiders or sympathizers. It is a common misperception to believe that ideological considerations will prevent terrorists from accepting assistance or coordinating activities with terrorists or states on the opposite side of the religious or political spectrum. Quite often terrorists with differing ideologies have more in common with each other than with the mainstream society they oppose. Common ideological categories include:

(1) **Political.** Political ideologies are concerned with the structure and organization of the forms of government and communities. While observers outside terrorist organizations may stress differences in political ideology, the activities of groups that are diametrically opposed on the political spectrum are similar to each other in practice.

(a) **Reactionaries.** Any political movement that seeks a return to a previous state (the status quo ante) and opposes changes in society it deems harmful. Today the term is largely used pejoratively to refer to those with ideas that are considered backwards, outdated, and opposed to "progress."

(b) **Fascist.** A movement that combines radical and authoritarian nationalist political ideology and a corporatist economic ideology. They believe that nations and/or races are in perpetual conflict whereby only the strong can survive by being healthy, vital, and by being assertive in conflict against the weak. Fascists advocate the creation of a single-party state and forbid and suppress criticism and opposition to the government and the fascist movement.

(c) **Socialist.** A movement advocating state, public, or common worker (e.g., through cooperatives) ownership and administration of the means of production and

distribution of goods, and a society characterized by equal access to resources for all individuals with an egalitarian method of compensation.

(d) **Communist.** A movement with political ideas and social movements related to the establishment of an egalitarian, classless, or stateless society based on common ownership and control of the means of production and property in general, as well as the name given to such a society. Those seeking a form of government in which the state operates under a one-party system and declares allegiance to Marxism-Leninism or a derivative thereof.

(e) **Neo-Nazism.** A political movement or ideology seeking to revive Nazism or some variant that is based on core aspects of Nazism such as socialist authoritarianism with racial or ethnic nationalist overtones. Neo-Nazis rarely use the word *neo-Nazi* to describe themselves, often opting for labels such as *national socialist*, *nationalist*, or related terms.

(f) **Anarchist.** Anarchist groups are anti-authority or anti-government, and strongly support a form of individual liberty that is disassociated from any form of government and voluntary association of cooperative groups. Often blending anti-capitalism and populist or communist-like messages, modern anarchists tend to neglect the problem of what will replace the current form of government, but generally promote that small communities are the highest form of political organization necessary or desirable. Currently, anarchism is the ideology of choice for many individuals and small groups who have no particular dedication to any ideology, and are looking for a convenient philosophy to justify their actions.

(2) **Religious.** All of the major world religions have extremists that have taken up violence to further their perceived religious goals. Religiously motivated terrorists see their ultimate objectives as divinely sanctioned, and therefore infallible and nonnegotiable.

(a) Religious motivations can also be tied to ethnic and nationalist identities, such as Kashmiri separatists combining their desire to break away from India with the religious conflict between Islam and Hinduism. The conflict in Northern Ireland also provides an example of the mingling of religious identity with nationalist motivations. There are frequently instances where groups with the same general goal, such as Kashmiri independence, will engage in conflict over the nature of that goal (religious or secular government).

(b) Of particular concern to US interests are transnational terrorist groups, such as al-Qaeda and its affiliates, who unite based on narrow religious interpretations regardless of ethno-national identity and who espouse the destruction of the US and its allies and partners. These groups tap into particular religious motivations to support political aims, such as the establishment of radical Islamic governments and the removal of Western influences.

(c) Numerous religious groups have either seen activists commit terrorism in their name, or spawned cults professing adherence to the larger religion while following

unique interpretations of that particular religion's dogma. Cults that adopt terrorism are often apocalyptic in their worldview. These groups are dangerous, unpredictable, and difficult to penetrate or deter. The Aum Shinrikyo sarin gas attack on the Tokyo Subway in 1995 illustrates the potential threat posed by such groups.

(3) **Social.** Often particular social policies or issues will be so contentious that they will incite extremist behavior and terrorism. Frequently this is referred to as “single issue” or “special interest” terrorism.

c. **Geographic Categories.** Geographic designations are sometimes used to categorize terrorist groups, although they are often confusing. In some instances geography overlaps ethnic, national, and religious/ideological aspirations. In other instances it is less relevant when referring to international and transnational terrorism. Often, a geographical association to the area with which the group is primarily concerned will be made. “Middle-Eastern” is an example of this category, and came into use as a popular shorthand label for Palestinian and Arab groups in the 1970s and early 1980s. Frequently, these designations are only relevant to the government or state that uses them. However, when tied to particular regions or states, the concepts of domestic and international terrorism can be useful.

(1) **Domestic or Indigenous.** These terrorists are “home-grown” and typically operate within and against their home country. They are frequently tied to extreme political, religious, or social factions within a particular society and focus their efforts specifically on their nation's sociopolitical arena. Domestic or indigenous terrorists often receive terrorist training or tactical experience abroad and return home with the intent to advance their terrorist agenda.

(2) **International.** Often describing the support and operational reach of a group, this term and transnational are often loosely defined, and can be applied to widely different capabilities. International groups typically operate in multiple countries, but retain a geographic focus for their activities. For example, Hezbollah has cells worldwide and has conducted operations in multiple countries, but is primarily concerned with events in Lebanon and Israel. Note: An insurgency-linked terrorist group that routinely crosses an international border to conduct attacks, and then flees to safe haven in a neighboring country, is “international” in the strict sense of the word, but does not compare to groups that habitually operate across regions and continents.

(3) **Transnational.** Transnational groups operate internationally, but are not tied to a particular country, or even region. Al-Qaeda is transnational, being made up of many nationalities, being based out of multiple countries simultaneously, and conducting operations throughout the world. Their objectives affect dozens of countries with differing political systems, religions, ethnic compositions, and national interests.

5. State Affiliation

a. Categorizing terrorist groups by their affiliation with states provides analysts indicators of their potential capabilities and targeting. Capabilities include the level and type of training, intelligence, logistic and operational support, funding, equipment, and weaponry. State affiliation may also be an indicator of probable targets and even preferred TTP. A terrorist group's selection of targets and tactics is also a function of the group's affiliation, level of training, organization, and sophistication. Joint doctrine identifies three types of state affiliations: **non-state supported**, **state supported**, and **state directed terrorist groups** (see 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 “non-state 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 servitude), or “state directed” (e.g., Hezbollah is both the “Party of God” and a religious organization that employs violence in support of both religion and politics).

c. Transnational terrorism is essentially conducted by a network of networks comprised of extremist organizations, ideological motivated state and non-state actors, and other opportunists or extremists who cooperate out of self-interest. They may not agree explicitly with the terrorists or their goals or methods, but expect to achieve some benefit or profit

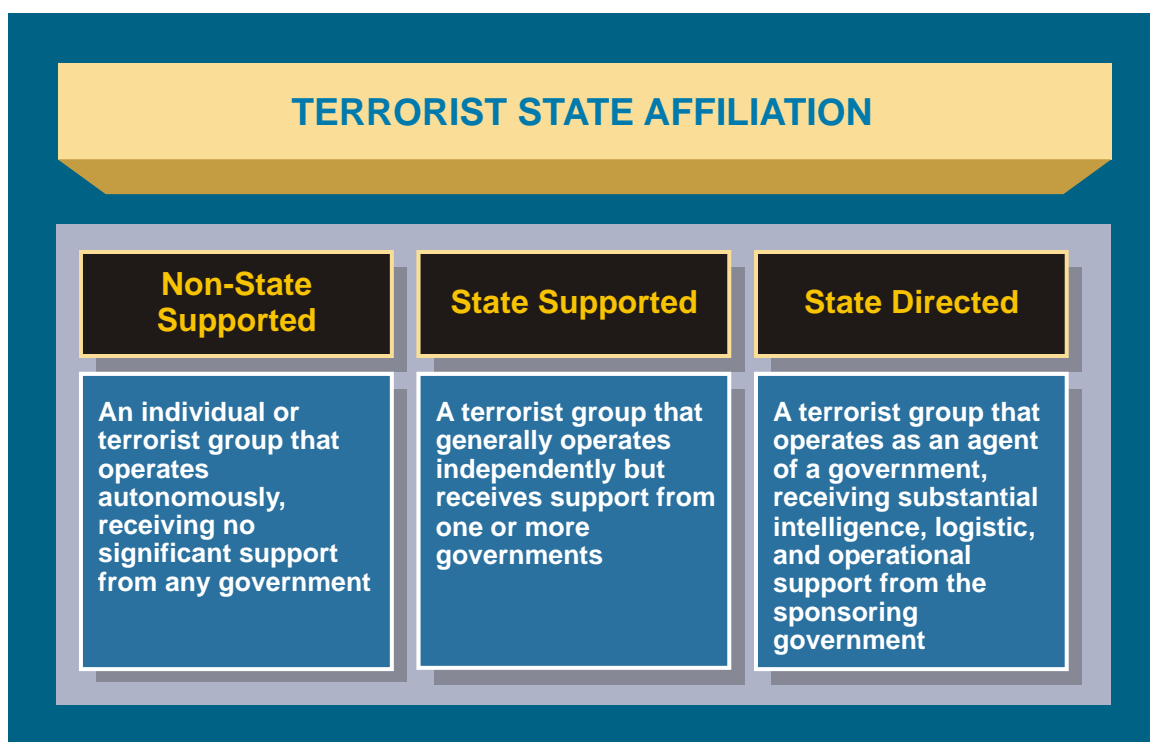


Figure II-1. Terrorist State Affiliation

from their cooperation with the terrorists. These opportunists and radicals include criminals, organized crime, weapons proliferators, rogue states, and insurgent groups who are key enablers to terrorists.

6. Terrorist Membership

a. **Levels of Commitment.** Typically, there are four different levels of commitment within a terrorist organization: **leadership, cadre, active supporters, and passive supporters.**

(1) **Leaders** provide direction and policy, approve goals and objectives, and produce overarching guidance for operations. Leaders may rise from within the ranks of an organization or create their own organization.

(2) **Cadre** are the zealots of a terrorist organization who not only plan and conduct operations, but also manage technology, intelligence, finance, logistics, IO, and communications. Mid-level cadres tend to be trainers and technicians such as bomb makers, financiers, and surveillance experts. **Low-level cadres are the bombers and direct action terrorists for other types of attacks.**

(3) **Active supporters** participate in the political, fund-raising, and information activities of the group. Acting as an ally or tacit partner, they may also conduct initial intelligence and surveillance activities, and provide safe houses, financial contributions, medical assistance, and transit assistance for active cadre members in more of a logistical role. **Usually, they are fully aware of their relationship to the terrorist group but do not commit violent acts.**

(4) **Passive supporters** are typically individuals or groups that are sympathetic to the announced goals and intentions of the terrorist organization, but are not committed enough to take action. Passive supporters may interact with a front group that hides the overt connection to the terrorist group, or passive supporters may intermingle with active supporters without being aware of what their actual relationship is to the organization. Sometimes fear of reprisal from terrorists compels passive support. Sympathizers can be useful for political activities, fund-raising, and unwitting or coerced assistance in intelligence gathering or other nonviolent activities.

b. Recruiting

(1) Terrorist groups recruit from populations that are sympathetic to their ideology and objectives. Often legitimate organizations can serve as recruiting grounds for terrorists. For example, militant Islamic recruiting has been linked to the schools (i.e., *madrassas*), established by radical Islamist clerics.

(2) **Capabilities.** Some recruiting may be conducted on the basis of particular skills and qualifications, rather than ideological characteristics. Of particular concern are attempts to recruit personnel with CBRN experience. Another concern is the recruitment of current or former members of the US and partner nation armed forces, both as trained

operatives and as agents in place. Recruiters target groups that feel disenfranchised, such as prisoners, the unemployed, the poor, and immigrants.

(3) **Coercion.** Through coercion, recruiters can gain operatives from diverse backgrounds. Some groups will also use coercion and leverage to gain limited or one-time cooperation from useful individuals. This cooperation can range anywhere from gaining information to conducting a suicide bombing operation. Blackmail and intimidation (e.g., threats to family members) are the most common forms of coercion and are often directed at personnel in government security and intelligence organizations.

c. **Tactical Level Cellular Organization.** The smallest elements of terrorist organizations are the cells at the tactical level—the building blocks for the terrorist organization. **One of the primary reasons for a cellular or compartmental structure is security.** A cellular structure makes it difficult for an adversary to penetrate the entire organization, and the compromise or loss of one cell does not compromise the identity, location, or actions of other cells. Personnel within one cell may not be aware of the existence of other cells or their personnel and, therefore, cannot divulge sensitive information to infiltrators or captors. Terrorists may organize cells based on tribal, family, or employment relationships, on a geographic basis, or by specific functions such as direct action or intelligence. Some cells may be multifunctional. The terrorist group uses the cells to control its members. Cell members remain in close contact with each other in order to provide emotional support and to prevent desertion or breach of security procedures. The cell leader is normally the only person who communicates and coordinates with higher levels and other cells. Thus, a local terrorist group could, unwittingly, be part of a larger transnational or international network.

d. **Proliferation of Information Between Organizations.** Terrorist groups increase their capabilities through the exchange of experience and knowledge by providing information to one another. Military professionals must evaluate potential terrorist threats according to what capabilities they may acquire through known or suspected associations with other groups, or those capabilities that can be acquired through the study and employment of techniques and approaches that have proven successful for other terrorist organizations. These exchanges occur both directly and indirectly. Direct exchange occurs when one group provides the other with training or experienced personnel not readily available otherwise.

(1) An example of direct exchange is the provision of sophisticated bomb construction expertise by the IRA to less experienced groups. In 2001, three members associated with the IRA were arrested in Colombia for inter-group terrorist support in use of explosives and other terrorist techniques. Terrorism techniques not previously observed as a norm in FARC [Revolutionary Armed Forces of Colombia] operations, such as the use of secondary explosive devices, indicated a transfer of IRA tactics and techniques.

(2) To disseminate much of this knowledge, terrorist organizations often develop extensive training initiatives. Al-Qaeda, for instance, has assembled in excess of 10,000 pages of written training material, more than 100 hours of training videos, and a global

network of training camps, and training material can be distributed in both hard copy or via the Internet.

(3) Indirect transfer of information/knowledge occurs when one group carries out a successful operation and is studied and emulated by others. The explosion of hijacking operations in the 1970s, and the similar proliferation of hostage taking in the 1980s were the result of terrorist groups observing and emulating successful techniques. The widespread use of improvised explosive devices (IEDs), vehicle-borne IEDs (VBIEDs), and suicide bombers are further examples of emulated successes.

7. Common Terrorist Tactics, Techniques, and Procedures

Terrorists employ a variety of TTP—some small scale, some large scale—to produce fear in their intended audience. Their targets may be just as likely economic (tourists, financial networks) or agricultural (livestock, crops), as they are embassies or military forces. Their goal is not just to win favor for their causes, but to erode the confidence, capability, and legitimacy of the government or societies they wish to coerce. The term terrorism is often used interchangeably with the term insurgency. Indeed, several of the tactics discussed in this section may also be used in an insurgency. An insurgency involves the use of subversion and violence by a group or movement that seeks to overthrow or force change of a governing authority. Insurgents use a variety of tactics, including terrorism, guerrilla warfare, and even conventional warfare. What typically distinguishes terrorism is that while both terrorism and insurgency seek political aims, terrorism is always unlawful and specifically intended to inculcate fear to achieve its aims. The most common TTP employed by terrorist groups are discussed below.

For more information on insurgency, refer to JP 3-24, Counterinsurgency Operations.

a. **Assassination.** An assassination is a deliberate action to kill specific, usually prominent, individuals such as political leaders, notable citizens, collaborators, or particularly effective government officials, among others. A terrorist group will assassinate people it cannot intimidate, those who have left the group, people who support the “enemy,” or people who have some symbolic significance to the enemy or world community. Terrorist groups may refer to these killings as “punishment” or “justice” as a way of legitimizing them. Assassinations are an effective psychological tool of terrorist tactics.

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. It is most often used for symbolic attacks and to create economic effects.

c. **Bombing.** The 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. Another common method of attack is suicide bombings. 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. **Kidnapping and Hostage Taking.** Kidnapping is the unlawful seizure and captivity of one or more individuals. Kidnappings usually result in the individual being held hostage in order to extract specific demands, but may be for intelligence gathering or execution. A successful kidnapping usually requires elaborate planning and logistics. Similarly, hostage taking is the seizure of one or more individuals usually overtly, with the intent of gaining advantage: publicity, ransom, political concessions, and release of prisoners. Targets of terrorist related kidnappings and hostage taking are usually prominent individuals such as high ranking foreign diplomats or officers; or of symbolic value such as government, military, or law enforcement personnel; foreign businesspeople; or tourists. Because the perpetrator may not be known for a long time, the risk to the perpetrator is less than in the overt hostage situation. Hostages can also serve as human shields, increasing terrorists' chances of success in carrying out a mission or to use in exchange for other government detainees or prisoners. While dramatic, hostage and hostage barricade situations are risky for the perpetrator. Killing of hostages may occur once the terrorist group believes that it has fully exploited the media coverage from the situation.

e. **Hijacking.** Hijacking involves the forceful commandeering of a mode of conveyance. Normally associated with aircraft—often referred to as skyjacking—it may also include ships, trains, or other forms of conveyance. Hijacking normally is carried out by terrorists to produce a spectacular hostage situation or provide a vehicle for carrying out a lethal mission (e.g., using an aircraft as a weapon), but is also employed as a means of escape.

f. **Seizure.** Seizure usually involves occupying and holding a prominent building or object of symbolic value (e.g., a US embassy, DOD Web site, or cyberspace node). There is usually considerable risk to the terrorist because security personnel have time to plan and react. Security personnel are more likely to use force to resolve the incident, if few or no innocent lives are involved.

g. **Raids or Ambushes.** A terrorist raid is similar in concept to a conventional military operation, but usually is conducted with smaller forces against targets marked for destruction, hijacking, or hostage/barricade operations. In some cases, the raid is designed to allow control of the target for the execution of another operation. An ambush is a surprise attack characterized by violent execution and speed of action.

h. **Sabotage.** Sabotage is defined as deliberate action aimed at weakening another entity through subversion, obstruction, disruption, and/or destruction. The objective in most sabotage incidents is to demonstrate how vulnerable society and its critical infrastructure are to terrorist actions and the inability of the government to stop terrorism. 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 attracts immediate public and media attention. Military facilities and installations, information systems, commercial industry, human resources, and



Port facilities may be one target of terrorist attacks.

energy and communication infrastructures are examples of attractive targets of terrorist sabotage.

i. **Threats or Hoaxes.** Any terrorist group that has established credibility can employ a hoax with considerable success. A credible threat causes time and effort to be devoted to increased security measures. A bomb threat can close a commercial building, empty a theater, or delay an aircraft flight at no cost to the terrorist. Threats may also be used by terrorists to probe and observe security procedures. Repetitive or an inordinate number of false alarms may dull the analytical and operational efficiency of key security personnel, thus degrading readiness. For more discussion, see Chapter III, “Intelligence.”

j. **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. For example, possible tactics may include the intentional dumping of hazardous chemicals into the public water supply, poisoning or destroying a nation’s food supplies through introduction of exotic plants or animals, destroying oil fields, or attacking an oil tanker to cause ecological harm. The use of exotic insects, animals, or plants to poison or damage the food supply or ecosystem is a potential low-cost weapon.

8. Terrorist Use of Asymmetrical Tactics

Terrorists prefer to attack their adversaries asymmetrically by circumventing an opponent’s strength and exploiting his weaknesses. Using this approach, terrorists pick the time, place, and manner of the attack while avoiding direct contact with their targets. Notably, these methods constantly evolve and often vary according to target and terrorist

cell. The following provides descriptions of asymmetric tactics routinely employed by terrorist adversaries.

a. Denial and Deception

(1) **Dispersing and Hiding.** Dispersion and hiding in complex terrain and urban environments degrade situational awareness and complicate US intelligence and targeting efforts. Urban areas offer excellent cover and concealment from US ground and airpower because building interiors and subterranean areas are hidden from airborne observation and vertical obstructions hinder line of sight to ground targets.

(2) **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.

(3) **Ruse.** Terrorists also use police cars, taxis, and ambulances to move couriers, fighters, and ammunition. Terrorist forces have used civilian vehicles configured as VBIEDs as “technicals” to maneuver and fight, and as supply and transport vehicles. In one example, enemy forces reconfigured a white van into a VBIED with red crescents painted on the front and sides (similar to impersonating an American Red Cross vehicle), which was later detonated near a local hotel.

b. Human Shields

(1) In their attacks, terrorists deliberately use civilians as human shields. This tactic forces friendly forces to adopt more stringent rules of engagement (ROE).

(2) Terrorists purposefully conduct operations in close proximity to civilians. 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.

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

(4) Attack targets from residential areas. Terrorists have launched attacks from residential areas in order to invite return fire into civilian homes.

c. Ambush and Surprise Attacks

(1) In general, terrorists avoid or desire to limit their direct fire engagements with heavy armored vehicles and prefer to conduct “standoff” attacks with IEDs 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.

(2) **“Shoot and Scoot” Tactics.** Mortars and rockets are the primary weapons of choice used by terrorists 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 “scooting” to a new location. Terrorists also leave these systems behind for capture after firing to avoid counterbattery fire. 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.

(3) **Stand-off Weaponry.** Mortars, rockets, 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 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.

(4) **Attacking 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. Such attacks undermine the government’s efforts to maintain stability and attempt 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 below.

(5) **Improvised Explosive Devices.** An IED is 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. IEDs have become a favored weapon of insurgents and terrorists because they can be fabricated at low cost with readily available materials, are easy to place and difficult to detect, and they generate publicity.

(6) **Explosively Formed Projectiles (EFPs).** Another popular weapon used in terrorist attacks, the EFP is a type of IED designed primarily to defeat vehicle armor by incorporating an explosive main charge with a machined or pressed concave metal plate that is reshaped into a high velocity metal slug capable of penetrating armor when the device is detonated.

(7) **Suicide-bomber attacks.** Suicide bombers are favored for their ability to precisely control the time and place of the explosion. Suicide bombers are the delivery vehicles and triggering devices for the explosives they are transporting with the added benefit of demoralizing the opponent by proving the extreme commitment to their cause. 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.

d. **Information Operations.** Terrorists have used IO to disrupt popular support for coalition forces and to garner regional and international sympathy and support for insurgent forces, mainly from Europe and the Islamic world. Terrorists are adept at disseminating information quickly thus putting friendly IO in a defensive posture. IO TTP include:

(1) **Spreading rumors on the “street.”** Rumors have always been a powerful force. News from the marketplaces and cafes has always been used to offset official information. Terrorists plant many rumors and initiate disinformation to discredit information from partner nations and the United States Government (USG). 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. Rumors in Operation IRAQI FREEDOM (OIF), which took months to disprove, included the distribution of disease-laden toys by coalition soldiers to Iraqi children and the harvesting of human organs by US soldiers for sale on the Internet.

(2) **Releasing favorable combat footage.** Terrorists rely heavily on video to distribute their propaganda. For example, crude digital video discs (DVDs) containing footage of attacks on multinational forces, wounded women and children, and damaged local infrastructure may appear in regional marketplaces immediately after attacks. DVDs will usually praise the bravery of residents “who didn’t submit to humiliation by the Americans,” and include scenes depicting the bravery of fighters as they engage multinational forces.

(3) **Posting video on the Internet.** Terrorists can use the Internet to disseminate their 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 terrorists and to create special effects or deception. Video footage of terrorist successes are used for recruitment and to sustain morale. Multimedia sites display manufactured evidence of USG and allied “atrocities and war crimes” to turn domestic and international opinion against the USG.

(4) **Ensuring media access.** Terrorists 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.

9. Terrorism Against the Homeland

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 Nation.

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 asymmetric 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.

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.

See JP 3-27, Homeland Defense, and JP 3-28, Civil Support, for guidance in the conduct of HD operations.

CHAPTER III INTELLIGENCE

“The struggle against international terrorism places new and difficult demands on the US Intelligence Community. Acquiring information about the composition, location, capabilities, plans, and ambitions of terrorist groups is an enormous challenge for intelligence agencies; meeting this challenge requires different skills than were needed to keep informed about the capabilities and intentions of Communist governments.”

**Congressional Research Service Report for Congress
Intelligence to Counter Terrorism: Issues for Congress
21 February 2002**

1. Role of Intelligence

This chapter highlights the importance of intelligence to AT activities. In particular to AT programs, intelligence is a key component to developing accurate, timely, and relevant threat assessments for risk management purposes.

a. **Intelligence in AT.** Accurate, timely, and relevant intelligence is critical in identifying and assessing terrorist capabilities, plans, intent, emerging trends, magnitude, probable courses of action, and possible targets. Each intelligence discipline contributes to AT capabilities through the use of signals intelligence (SIGINT), geospatial intelligence (GEOINT), measurement and signature intelligence, human intelligence (HUMINT), and open-source information. By integrating all available sources of intelligence, commanders have the basis for the development of an effective AT program. The ability of the intelligence enterprise to provide critical, relevant, and timely information to the user depends not only on efficient collection, processing, and exploitation, but also on the ability to organize, store, and rapidly retrieve, fuse, and disseminate this information. This capability, drawing from federal, state, local, and international sources, increases the probability of accurately predicting the types and timing of terrorist attacks and allows commanders to develop threat assessments as part of the risk assessment process.

b. **USG Intelligence Structure.** In order to increase information sharing and facilitate the production of an integrated, all-source intelligence product, the Director of National Intelligence (DNI) oversees the intelligence community (IC) and is responsible for integrating foreign, military, and domestic intelligence in defense of the homeland and of US interests abroad. The following is a brief summary of some of the members of the IC:

(1) **The National Counterterrorism Center (NCTC)** is the primary USG organization responsible for integrating and analyzing all intelligence possessed or acquired pertaining to terrorism, with the exception of purely domestic terrorism.

(2) **The Defense Intelligence Agency’s (DIA’s) Defense Intelligence Operations Coordination Center** is the lead DOD intelligence organization responsible for integrating

and synchronizing military intelligence and national intelligence capabilities in support of the combatant commands.

(3) DIA's **Joint Intelligence Task Force - Combating Terrorism (JITF-CT)** serves as the single, national-level, all-source foreign terrorism intelligence effort and repository within DOD, and as the DOD focal point for analysis of data information pertaining to domestic and foreign terrorist threats to DOD elements and personnel (excluding threats posed by US persons who have no foreign connection).

(4) The DNI's **Open Source Center** coordinates and integrates open-source intelligence into IC products.

(5) The **Federal Bureau of Investigation (FBI)** leads IC efforts on the prevention of domestic terrorism.

(6) The **Central Intelligence Agency (CIA)** deals primarily with HUMINT collection, all-source analysis, and the production of political, economic, and biographic intelligence.

(7) The **National Geospatial-Intelligence Agency** provides a broad range of GEOINT support, such as persistent surveillance, mapping, and imagery support, for the planning and execution of AT. For additional information, see JP 2-03, *Geospatial Intelligence Support to Joint Operations*.

(8) The **National Security Agency** focuses on protecting US national security systems and the production of foreign SIGINT information.

For additional information on the IC, refer to JP 2-0, Joint Intelligence, and JP 2-01, Joint and National Intelligence Support to Military Operations.

c. **Legal Considerations and Intelligence.** There are several regulations, executive orders, and laws that specifically govern the use of DOD intelligence assets and organizations in domestic operations. The purpose of the DOD Intelligence Oversight program is to ensure that military intelligence personnel do not improperly collect, retain, or disseminate information about US persons and corporations. However, this does not affect counterintelligence collection. Commanders and their intelligence staffs should be fully cognizant of their intelligence oversight responsibilities. Intelligence regarding US citizens in particular must be done in accordance with specific guidelines. For more information on legal considerations during DOD intelligence activities in domestic operations or against US persons, see Chapter IV, "Legal Considerations"; DODD 5240.01, *DOD Intelligence Activities*; DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons*; DODD 5525.5, *DOD Cooperation with Civilian Law Enforcement Officials*; DODD 5200.27, *Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense*; and EO 12333, *United States Intelligence Activities*, as amended.

2. Intelligence and Risk Management

The AT program is a comprehensive effort focused on the detection and prevention of terrorist attacks against DOD personnel, their families, installations, and supporting infrastructure critical to mission accomplishment. This includes the planning and preparation to respond to terrorist incidents. Intelligence provides the commander with a threat analysis that reviews the factors of a terrorist group's operational capability, intentions, and activity, as well as the operating environment within which friendly forces operate. Commanders must carefully exercise judgment in estimating both the existing terrorist threat and the need for changes in AT measures (see Appendix E, "Risk Management Process").

a. **Risk Management.** 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. This requires an RA. An RA is determined by combining a TA, VA, and criticality assessment (CA) in order to provide a commander with a more complete picture of the risks facing an asset or group of assets. The TA is based on a threat analysis of the full range of enemy capabilities and intentions; it 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 VA is an evaluation to determine the vulnerability to a terrorist attack against an installation, unit, exercise, port, ship, residence, facility, or other site. A CA identifies key assets and infrastructure that are deemed mission critical; it addresses the impact of temporary or permanent loss capability to include costs of recovery and reconstitution. When conducting an RA, the commander and staff must carefully exercise judgment in estimating both the existing terrorist threat and the need for changes in AT measures.

b. **Intelligence Resources for Threat Assessments.** DIA maintains the Combating Terrorism Database (CTDB) and a corresponding Web site called the Combating Terrorism Knowledge Base (CTKB). The intelligence directorate of a joint staff (J-2) at the combatant command level, in consultation with DIA, focuses this database information and other regional information toward the intelligence needs specific to the security of the command. Country TAs and information about terrorist organizations, biographies, and incidents in the database are updated and available on the CTKB Web site. Commands at all echelons then augment or refine the DIA's analyses to focus on their area of interest. This process is implemented across the range of military operations and promotes both coordination among all levels of the IC and LE, and enhances timely distribution of information to the supported commander. In addition, Defense Threat Reduction Agency (DTRA) performs threat assessments, provides training, and assists in threat reduction planning, particularly against WMD.

c. **AT Intelligence Challenges.** Several factors complicate AT intelligence collection and CI activities. The majority of terrorist groups are small, mobile, and organized using cell-like structures. These attributes make it difficult to identify and target the members and their assets. Unlike other criminal groups, terrorist cadres often receive training in CI, OPSEC, and security measures from foreign intelligence agencies or other terrorist groups. Individual terrorists are difficult to identify, complicating any information gathering or

intelligence analysis, to include determining extant capabilities and their most likely and dangerous courses of action. AT requires additional proactive efforts that integrate the traditional LE measures with intelligence analysis. AT officers and analysts may want to maintain a threat information organization plan that systematically outlines threats and threat indicators.

d. **AT Intelligence 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 detect and respond. Drills and exercises test suspected vulnerabilities and AT intelligence processes. 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 and known vulnerabilities.

For more information on threat assessment, see Appendix A, “Antiterrorism Plan,” Appendix E, “Risk Management Process,” and DODD 2000.12, DOD Antiterrorism (AT) Program.

3. Intelligence Support

a. **Intelligence Support.** Well-planned, proactive, systematic, all-source intelligence provides decision makers with information and timely warnings upon which to recommend FP actions and build an effective AT program. An effective AT program contributes to disruption of threat incidents through preventive measures and includes proactive and reactive phases. During the proactive phase, organizations perform threat and intelligence analysis, conduct information sharing, and compile CAs and VAs in order to develop a comprehensive TA. During the reactive phase, organizations perform crisis management actions and execute the commander’s AT intent.

b. **Factors.** A comprehensive TA may reveal weaknesses in day-to-day operations. Various security disciplines and factors must be examined and weaknesses corrected in order to mitigate risks. OPSEC, personnel security, physical security, and information security programs must focus on denying information and increasing the risk to the threat.

c. **Process.** The intelligence process is continuous throughout operations. It involves planning and direction; collection; processing and exploitation; analysis and production; dissemination and integration; and evaluation and feedback. Detecting terrorism’s asymmetric methods of operation requires a higher level of situational understanding, based on continuous intelligence support. This threat drives the need for predictive intelligence based on analysis of focused information from all sources.

d. **Intelligence Preparation of the Battlespace (IPB).** IPB is a systematic approach to analyzing the threat and the environment in a specific geographic area. Well-developed IPB products and analysis help identify facts and assumptions about the installation, relevant terrain, and the threat. The application of IPB in AT operations must be especially fluid, flexible, and creative. Organizations must be prepared to combine or discard various techniques to suit the situation and provide the commander with a product that will aid in the decision-making process.

e. **Sources.** All-source intelligence should be used as the basis for an AT program including: open-source information; local, state, and federal LE information; national-level intelligence; information shared through liaison with foreign governments; biometrics and forensics exploitation data; and military source operations in some overseas deployed environments (see Figure III-1). Biometric information and the use of forensic tools and



Figure III-1. Sources of Intelligence

procedures limit the ability of the enemy to remain anonymous and hide among the civilian population. This data can be used to locate and track terrorist and support networks.

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

(1) **Open-Source Intelligence.** This information is publicly available and can be collected, retained, and stored by the IC. Collection activities by intelligence components that affect US persons must be accomplished in accordance with DOD 5240.1-R, *Procedures Governing the 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 an excellent source of terrorism information and often include in-depth reports on individuals, groups, or various government counterstrategies. Other nongovernment sources include commercial and academic think tanks that maintain online databases, libraries, and current research. Government sources include congressional hearings; publications by the FBI, CIA, DIA, DOS, the DNI Open Source Center, the Department of Justice (DOJ), the Department of the Treasury, the Department of Homeland Security (DHS); 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.

(2) **Law Enforcement Information.** Both military and civil law enforcement agencies (local, state, and federal) have access to criminal records. Because terrorist acts are often prosecuted as criminal acts, both in the US and overseas, criminal records can be an important source of intelligence. Because the collection, retention, and dissemination of criminal records are regulated, DOD utilizes established LE liaison channels. LE liaisons have the ability to provide DOD organizations with relevant information from criminal records while preserving the evidentiary value of that information. 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 may assist in determining the local terrorist threat. Similarly, the DOD's Biometrics Task Force maintains robust information sharing relationships with the FBI and DHS to support biometric identification and screening operations. Personnel responsible for AT and LE personnel should maintain close contact and share information as appropriate. 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) **Strategic Intelligence.** The NCTC serves as the central, shared knowledge bank for terrorism information. The NCTC also provides all-source AT intelligence support, develops AT-supportive information technology systems, establishes interagency connectivity and architectures, provides access to AT intelligence, and integrates and disseminates AT intelligence and information. The DIA's JITF-CT is the DOD primary

point of contact for the NCTC and the mission manager for combating terrorism issues. The FBI has a National Joint Terrorism Task Force (NJTTF) which includes numerous agencies, spanning the fields of intelligence, public safety, and federal, state, local, and tribal LE. The NJTTF collects, analyzes, and funnels terrorism information and intelligence from and to the regional joint terrorism task forces (JTTFs). The DOD is represented on the NJTTF 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, NCIS, Marine Corps Intelligence Activity, and AFOSI. For combatant commands, the director of intelligence or J-2 is responsible for supporting the combatant commander and operational and planning staffs and for obtaining, developing, and providing the necessary intelligence products and support required for planning and execution of assigned combatant command missions. Combatant command J-2 responsibilities also include analysis, collection management, and interagency coordination. In addition, the combatant command J-2 must develop intelligence policies and plans and support theater and component intelligence and collection requirements and priorities.

(4) **Information from Local, State, and Federal Personnel.** 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. Intelligence exchanges with local government agencies through cooperative arrangements can also augment regional information.

(5) **Biometrics, Forensics, and Document and Media Exploitation (DOMEX).** Biometrics, forensics, and DOMEX are increasingly important in the areas of CT, AT, and intelligence support—all critical areas in identifying known and suspected terrorists and protecting DOD personnel. DOD's growing biometrics and forensic program capabilities enable appropriate authorities to collect, analyze, correlate, and disseminate a variety of biometric data (e.g., finger and palm prints and voice, facial, and iris images). Biometric data, combined with biographic, contextual, and other identity-related intelligence, enables high-fidelity threat analysis and assessment. Biometric data are a key element leading to identity assurance or certitude and lifting the veil of anonymity surrounding terrorists and related actors.

(6) DOD has formed partnerships with the FBI, DHS, DOS, and the broader IC to leverage the considerable identity holdings of the USG. Information sharing among the DOD's Automated Biometric Identification System, the FBI's Integrated Automated Fingerprint Identification System, and programs run by DOS and DHS significantly improve our ability to identify and apprehend known or suspected terrorists seeking to gain access to overseas USG facilities and to maintain effective installation access control and defense in depth for the terrorist threat against bases and facilities in the United States. As these partnerships expand to our foreign partners, the ability of the biometrics enterprise to support a broad array of CT, AT, and intelligence missions at the strategic, operational, and tactical

levels will expand significantly. Properly harnessed, these proven capabilities are one of the most powerful tools available for preventing terrorist attacks.

4. Antiterrorism Intelligence Roles and Responsibilities

a. **National-level AT Intelligence Roles and Responsibilities.** Within the United States, the FBI is responsible for collecting and processing terrorist information to protect the US 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 executive orders (EOs), federal law, status-of-forces agreements (SOFAs), MOUs, and applicable Service regulations.

b. DOD-level AT Intelligence Roles and Responsibilities

(1) **DIA.** The Director, DIA, under the Under Secretary of Defense for Intelligence, is responsible for establishing and maintaining an international all-source terrorism intelligence fusion center, JITF-CT. The JITF-CT provides a wide range of terrorism intelligence for DOD components, to include indications and warnings, current intelligence, assessments, in-depth analysis, DOD terrorism threat assessments/levels, and the maintenance of a CTBD.

(2) **GCCs.** The GCC, through the J-2, joint intelligence operations center, command counterintelligence coordinating authority, and subordinate component commands' CI and AT organizations, and in consultation with DIA, CIA, US country team, and applicable HN authorities, compiles 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. GCCs may also set terrorism threat levels for specific personnel, family members, DOD contractors in accordance with DODI 3020.41, *Contractor Personnel Authorized to Accompany the US Armed Forces* units, installations, or geographic regions in countries within the GCC's AOR, using the definitions and criteria established by the Director, DIA.

(3) **Services.** 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. Each Military Department is responsible for the following:

- (a) Provide overall direction and coordination of the Service CI effort.
- (b) 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.
- (c) Provide Service commanders with information on terrorist threats concerning their personnel, facilities, and operations.

“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 DOD. 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][SDO/DATT][senior defense official/defense attaché]). 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 [SDO/DATT]) 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*

(d) Investigate terrorist incidents with the FBI or HN authorities looking for intelligence, CI, and FP-relevant information.

(e) Provide terrorist threat information in threat briefings.

(f) Conduct liaison with representatives from federal, state, local agencies (county, tribal, city), and if applicable HN agencies to exchange information on terrorists.

(g) 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.

(4) **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.

(a) Intelligence staff elements of commanders at all echelons have the following responsibilities:

1. Promptly report all actual or suspected terrorist incidents, activities, and indicators/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.

(b) 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.

(c) 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 investigative 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.

(d) Services, DOD agencies, and installations should submit suspicious activity reports through their chain of command.

(e) Commanders are responsible for the development and implementation of proactive defensive techniques to detect, deter, and defeat terrorists, particularly in support of DOD elements and personnel or activities conducted in areas designated with SIGNIFICANT or HIGH threat levels. These activities shall include, but are not limited to, in-transit forces, HRP, special events, and high-value military cargo shipments.

c. Information Requirements. To focus threat analysis, the intelligence staff identifies significant gaps in what is known about the adversary and other relevant aspects of the operational environment and formulates intelligence requirements (general or specific subjects upon which there is a need for the collection of information or the production of intelligence). All staff sections may recommend intelligence requirements for designation as priority intelligence requirements (PIRs)—a priority for intelligence support that the commander and staff need. The joint force commander (JFC) designates PIRs, which together with friendly force information requirements constitute the commander's critical information requirements. Based on identified intelligence requirements (to include PIRs), the intelligence staff develops more specific questions known as information requirements (those items of information that must be collected and processed to develop the intelligence required by the commander). A subset of information requirements that are related to and would answer a PIR are known as essential elements of information. A representative sampling of information requirements (IRs) for use when conducting analysis of terrorist groups is depicted in Figure III-2.



Figure III-2. Information Requirements

CHAPTER IV LEGAL CONSIDERATIONS

“To effectively detain, interrogate, and prosecute terrorists, we need durable legal approaches consistent with our security and our values...we will bring terrorists to justice.”

**National Security Strategy
May 2010**

1. General

This chapter is designed to provide 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 both the inherent authority and the responsibility to enforce security measures and to protect persons and property under their control. Commanders should consult with their legal advisors regularly when establishing their AT programs.

3. Limits of Civil Support

a. **General.** DOD is the lead agency for conducting overseas HD operations. However, against internal threats (e.g., domestic terrorism), DOD may be in support of DOJ or DHS and may conduct civil support operations for declared emergencies.

b. **Civil Support.** When providing support to civil authorities, DOD will do so as directed by the President or SecDef and consistent with laws, presidential directives, EOs, and DOD policies and directives. DOD resources may be provided when requested by civil authorities and approved by SecDef. In most cases, assistance is provided on a cost-reimbursable basis. When imminently serious conditions resulting from any civil emergency or attack exist and time does not permit prior approval from higher headquarters, local military commanders and responsible officials of other DOD components are authorized to take necessary action to respond to requests from civil authorities to provide immediate assistance to save lives, prevent human suffering, or mitigate great property damage. This constitutes a policy of authority to act, where time does not permit obtaining express approval. However, support should not be delayed or denied because of the inability or unwillingness of the requester to make a commitment to reimburse DOD.

c. 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.

For more information on legal considerations during civil support operations, see JP 3-28, Civil Support, and JP 3-41, Chemical, Biological, Radiological, and Nuclear (CBRN) Consequence Management.

4. Authority for Handling Terrorist Incidents

a. Commanders' Responsibilities Inside the United States and its Territories and Possessions

(1) Although the FBI has primary LE responsibility for investigating terrorist incidents inside the US (including its possessions and territories) and the DOD LE and IC have a significant role within their 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 attacks or incidents involving DOD personnel, facilities, or assets trigger the need for four separate but related activities:

- (a) Immediate response, containment, and resolution of an incident.
- (b) Cooperation with appropriate civilian LE authorities.
- (c) Investigation of an incident for various purposes, to include protection of the crime scene. (See Chapter VI, "Terrorist Incident Response," regarding evidence and apprehended personnel.)
- (d) 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. This includes notifying the military criminal investigative organization and DOD Criminal Investigative Task Force regarding acts of terrorism and war crimes. Primary responsibility for investigating many of the most serious crimes on USG property shall normally rest with the DOJ, except for US military installations, on which the local commander retains primary responsibility.

For further information regarding use of force by DOD personnel, refer to CJCSI 3121.01B, Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces. For further information regarding the arming of DOD security and LE 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.

(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. In addition to certain restrictions on direct DOD support to law enforcement, commanders should also be mindful of applicable restrictions and DOD guidance regarding the use of DOD intelligence components and nonintelligence components to support civil authorities in domestic activities. Relevant references include

DODD 3025.12, *Military Assistance for Civil Disturbance (MACDIS)*; DODD 3025.15, *Military Assistance to Civil Authorities*; DODD 5200.27, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense*; DODD 5240.1, *DOD Intelligence Activities*; DODD 5525.5, *DOD Cooperation with Civilian Law Enforcement Officials*; DODD 5525.07, *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*; and JP 3-28, *Civil Support*.

(4) In the event the FBI assumes jurisdiction, the DOJ shall be the primary federal agency for the purpose of concluding 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 and coordination of rules for the use of force (RUF) should be addressed as part of the request for assistance.

(5) Attacks on DOD personnel or assets within the United States and its territories and possessions that are not on 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. It is important to note that commanders should consult their legal advisors, HN authorities, and all international agreements and US regulations before implementing any course of action off the installation.

For more information on RUF in a domestic environment during civil support, see CJCSI 3121.01B, Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces, and JP 3-28, Civil Support.

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

(1) Although DOS has the primary responsibility for dealing with terrorism involving Americans abroad, DOD commanders have the inherent right 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 GCC for further reporting to DOS. The commander is responsible for incident response and containment in order to protect DOD personnel and property from immediate threat of injury. DOS has the primary responsibility for coordinating the political and diplomatic response to terrorism involving Americans abroad. The installation or vessel commander should also implement any provisions of the SOFA or other agreements between the US 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, DOJ, in coordination with

DOS, 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 the unit commander, in accordance with the specific guidelines of CJCSI 3121.01B, military members may exercise individual self-defense in response to a hostile act or demonstrated hostile intent. If US forces are 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 or action is taken under the authority of immediate response to save lives, 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. Memorandum of Understanding and Memorandum of Agreement

(1) Title 22, United States Code (USC), Section 4802, 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 GCCs 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—GCC or COM—in the most efficient and effective 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 GCC (and designated AT planning and response elements) may enter into Mutual Assistance Agreements with HN authorities. 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 prepare for the worst-case scenario by planning responses based on organic resources and local support available 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 services, federal, state, and local agencies; special operations forces; engineers; CBRN units; and explosive ordnance disposal (EOD). Often through agreements with HN authorities, MOAs are adapted to grant the US installation commander responsibility within (or inside) the installation boundary, with the HN having responsibility outside this boundary. 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 installation boundary. Although the installation commander may not have security responsibility "outside the wire," the commander still maintains a security interest. The installation commander must include exterior terrain, avenues of approach, threat capabilities (possession of stand-off weapons such as man-portable air defense system 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.

(4) In 2003, an MOU between DOS and DOD established force protection detachments (FPDs). The primary mission of an FPD is to support the in-transit force protection requirements according to priorities established by the GCCs when military criminal investigative and CI organizations are not present. FPD activities include, but are not limited to, preparing TAs and informational documents, coordinating with foreign LE and security officials, producing AT surveys, assessing route and travel threats, briefing antiterrorist and CI threats, assisting in investigations and operations, assisting in protective service operations, and serving as a point of contact in embassies for DOD CI and LE organizations.

For further information, see DODI 5240.22, Counterintelligence to Force Protection and Memorandum of Understanding (MOU) Between the Department of State, Bureau of Diplomatic Security and the DOD Counterintelligence Field Activity Regarding Force Protection Detachments, 9 May 2003.

5. United States Coast Guard

The United States Coast Guard (USCG) is the lead or primary agency for maritime homeland security (HS). As such, the USCG operates at all times as both an Armed Force of the United States (Title 14, USC, Section 1), and a law enforcement agency (Title 14, USC, Section 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 maritime critical infrastructure.

Additionally, the USCG will prepare for and, in the event of attack, conduct emergency response operations. When directed, as the supported or supporting commander, the USCG will conduct military HD operations in its traditional role as a Military Service.

CHAPTER V

ANTITERRORISM PROGRAMS

“Al-Qaeda still plots and plans, especially in the border region between Afghanistan and Pakistan. It is the epicenter of global Islamic extremism, the origin of the 9/11 attacks and, should we be hit again, I am convinced the planning, training, and financing, as well as leadership, will emanate from there. That’s why we are so focused on it. That’s why we believe this mission is in our vital national-security interest and those of our allies and friends, and that’s why we are grateful for the contributions of the other nations committed to the fight.”

Admiral Michael Mullen
Chairman of the Joint Chiefs of Staff
8 Dec 2009

1. Antiterrorism Program Overview

a. Protection of DOD personnel and assets from acts of terrorism is one of the most complex challenges for commanders. AT programs consist of defensive measures to reduce the vulnerability of individuals and property to terrorist acts, including rapid containment by local military and civilian forces. An integrated and comprehensive AT program (physical security, construction standards, CBRN passive defense, OPSEC, CI, biometrics and forensics exploitation, etc.) must be developed, implemented, and updated in order to effectively detect, defend, and respond to a terrorist threat.

b. **AT Program Elements.** As a subset of the overarching FP program, the AT program is a collective, proactive effort focused on the prevention and detection of terrorist attacks against DOD personnel, their families, facilities, installations, and infrastructure critical to mission accomplishment as well as the preparation to defend against and planning for the response to the consequences of terrorist incidents. Important adjuncts to an effective AT program include plans for the initial response to a terrorist incident, as well as plans for continuing essential military operations. The minimum elements of an AT program are ***AT risk management, planning, training and exercises, resource management, and a program review.***

DODD 2000.12, DOD Antiterrorism (AT) Program, and DODI 2000.16, DOD Antiterrorism (AT) Standards, provide the specific requirements for these program elements.

(1) **Risk Management Process.** The risk management process is used in identifying, assessing, and mitigating risk arising from operational factors and making decisions that balance risk and cost with mission benefits. AT risk management allows the commander to decide how best to employ given resources and AT measures to deter, prevent, or mitigate a terrorist attack, balancing risk and cost while ensuring mission readiness. The risk management process consists of three key elements—***threat assessment, criticality assessment, and vulnerability assessment***—which are used to produce a final ***risk assessment***. Commanders may use the Risk Assessment Module in the Core Vulnerability Assessment Management Program (CVAMP) to help complete the risk assessment process.

(a) **Threat Assessment.** The terrorism TA determines the capabilities, intentions, and activity of terrorist organizations. Prescribed annual installation-level AT TAs are built by integrating threat information prepared by intelligence and LE communities. Tools, like the Under Secretary of Defense for Intelligence Defense Threat Assessment, are available as resources. The DIA's JITF-CT is the DOD focal point for the analysis of data and information pertaining to domestic and foreign terrorist threats to DOD personnel (excluding threats posed by US persons who have no discernable foreign control or connections). The JITF-CT also disseminates intelligence on foreign terrorist threats, including specific warning of threats against DOD personnel (including family members) and assets and is a starting point for any TA.

(b) **Criticality Assessment.** The CA provides the commander with a list of key assets and infrastructure based on the necessity for mission completion. Criticality is determined by the impact of loss on the mission. This can include physical infrastructure, HRP, as well as the Internet and computer systems. Critical assets will be identified and prioritized in accordance with DOD 3020.45-M, *Defense Critical Infrastructure Program (DCIP): DOD Mission-Based Critical Asset Identification Process (CAIP)*.

(c) **Vulnerability Assessment.** Vulnerability is determined by the level of susceptibility to attack by a broad range of terrorist threats against DOD personnel and assets. VAs for critical infrastructure should also address susceptibility to hazards (acts of nature, human error, etc.). Commanders conduct an annual VA and more often as circumstances warrant. The CVAMP is an online tool used to assess and prioritize vulnerabilities which can be accessed through ATEP.

(2) **AT Planning.** AT planning is the process of developing specific guidance, measures, and instructions to deter, mitigate, and prepare for a terrorist incident. The AT plan contains command-specific guidance to establish and maintain an AT program as outlined in DODI 2000.16, *DOD Antiterrorism (AT) Standards*. At a minimum, AT plans shall be developed at the installation, separate or leased facility or space, and ship levels, and also for operational deployments, training exercises or events, and special events. If applicable, AT plans can be synchronized with any existing installation emergency management plan while incorporating the assessments from the risk management process. AT principles should also be incorporated into all operation plans (OPLANs) and risk decisions to support the DOD components' unique roles and mission requirements. Additionally, stand-alone documents (e.g., standard operating procedures [SOPs], local regulations, and operations orders articulating requirements for these key elements) shall be replicated and/or referenced in the AT plan.

(3) **AT Training and Exercises.** An AT program must include training for development of individual, leader, and collective skills, and the conduct of comprehensive exercises to validate AT plans. AT training includes:

- (a) Annual exercise of AT plans.
- (b) Formal AT training (Levels I-IV for appropriate personnel).

- (c) AOR specific training.
- (d) Training for HRP and personal security detachment personnel.
- (e) Exercise documentation and process improvement/review.

(4) **Resource Management.** The PPBE process is the resource mechanism for identification of baseline and supplemental needs. Unfunded requirements to support a commander's mission (e.g., priority emergent requirements) can be submitted via the CCIF process.

(5) **Program Review.** A program review is required at least annually, during predeployment preparations and when significant changes occur regarding threat, asset criticality, or vulnerability. Commanders and component commands may use higher HQ assessments or Joint Staff Integrated Vulnerability Assessment (JSIVA) reports in lieu of annual AT program reviews.

2. Antiterrorism Plan Development

AT plans should prepare for the most likely threats and should maximize the use of existing plans and 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.

a. **AT Measures.** At a minimum, an AT plan must include measures that take into account the key elements of the AT program. AT measures should include random antiterrorism measures (RAMs), provisions for the use of physical structures, physical security equipment, CBRN detection and protection equipment, response forces, and other emergency response measures. All AT measures should be **scalable** and **proportional** to increases in the local threat and/or unit operational capability.

(1) Security measures, which improve situational awareness and present a robust FP posture, may serve to inhibit terrorist surveillance and deter targeting efforts. These measures can include:

- (a) Visible security cameras and motion sensors.
- (b) Working dog teams.
- (c) Active searches (including x-ray machines and explosive detection devices) of vehicles and persons at entry points.
- (d) Displays of vehicles mounted with crew served weapons.
- (e) Barriers, roadblocks, and entry mazes to increase standoff and improve security personnel reaction time during an attack.

- (f) Unmanned aerial systems.
- (g) Robust information access control TTP, to include cyberspace security.
- (h) Biometric and forensic data to screen personnel for identity and base access.
- (i) Electronic warfare systems to counter terrorist use of electromagnetic spectrum for remotely controlled IEDs, communications, and surveillance.

(2) **RAMs.** To be effective, RAM execution should be conducted for sufficient periods of time to increase the visibility and disruption of terrorist operational cycles. Enduring (or prolonged) RAMs will have a greater impact on an adversary's planning cycle. RAMs should be employed in conjunction with site-specific FPCON measures in a manner that portrays a highly visible and robust security posture from which terrorists cannot easily discern AT measures from security patterns or routines. Examples of RAMs include:

- (a) Irregular guard changes (time, number, location, TTP).
- (b) Roving security patrols varying in size, timing, and routes.
- (c) Surprise inspections and searches of personnel and vehicles.

More detailed information is available in the Joint Forward Operations Base (JFOB) Survivability and Protective Construction Handbook, and the Joint Entry Control Point and Escalation of Force Procedures (JEEP) Handbook.

b. **Risk Management Process.** As discussed above, the TA, CA, and VA are used to produce an over-all risk assessment. Use the final risk assessment as a guide to risk mitigation priorities and establish a local baseline or defense posture.

For more information, see Appendix E, "Risk Management Process."

c. **Physical Security.** Physical security measures incorporate facilities, equipment, trained personnel, and procedures into a comprehensive effort designed to provide optimal AT protection to personnel and assets. AT plans should include notifications to the appropriate emergency responders, including LE offices, and the servicing FBI field office enabling 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. Physical security measures should include or consider the following:

- (1) Construction standards and building considerations.
- (2) Critical asset security.
- (3) Coverage for off-base assets including infrastructure, facilities, housing, and activities.

(4) FPCON measures (see Figure V-1), which allow the commander to apply an operational decision to best protect personnel or assets from terrorist attack.

(5) Security for HRP.

(6) In-transit movements, logistics, and contracting.

d. **Incident Response.** Terrorist incident response ensures C2 communications and intelligence are provided to emergency responders charged with determining the full nature and scope of the incident, mitigating the damage, and countering any remaining terrorist(s). Terrorist incident response plans should include emergency response and disaster planning and/or preparedness to recover from a terrorist attack, to include CBRN attacks. A measure of deterrence may be achieved by demonstrating capabilities to respond to and mitigate the potential effects of terrorist attacks.

e. **Training and Exercises.** AT plans are exercised annually and whenever possible should be conducted in coordination with federal, local, state, tribal, or HN authorities and US embassies and consulates.

f. **AT Resource Management.** AT resource requirements can be identified via DOD's PPBE process, as well as available supplemental programs such as CCIF.

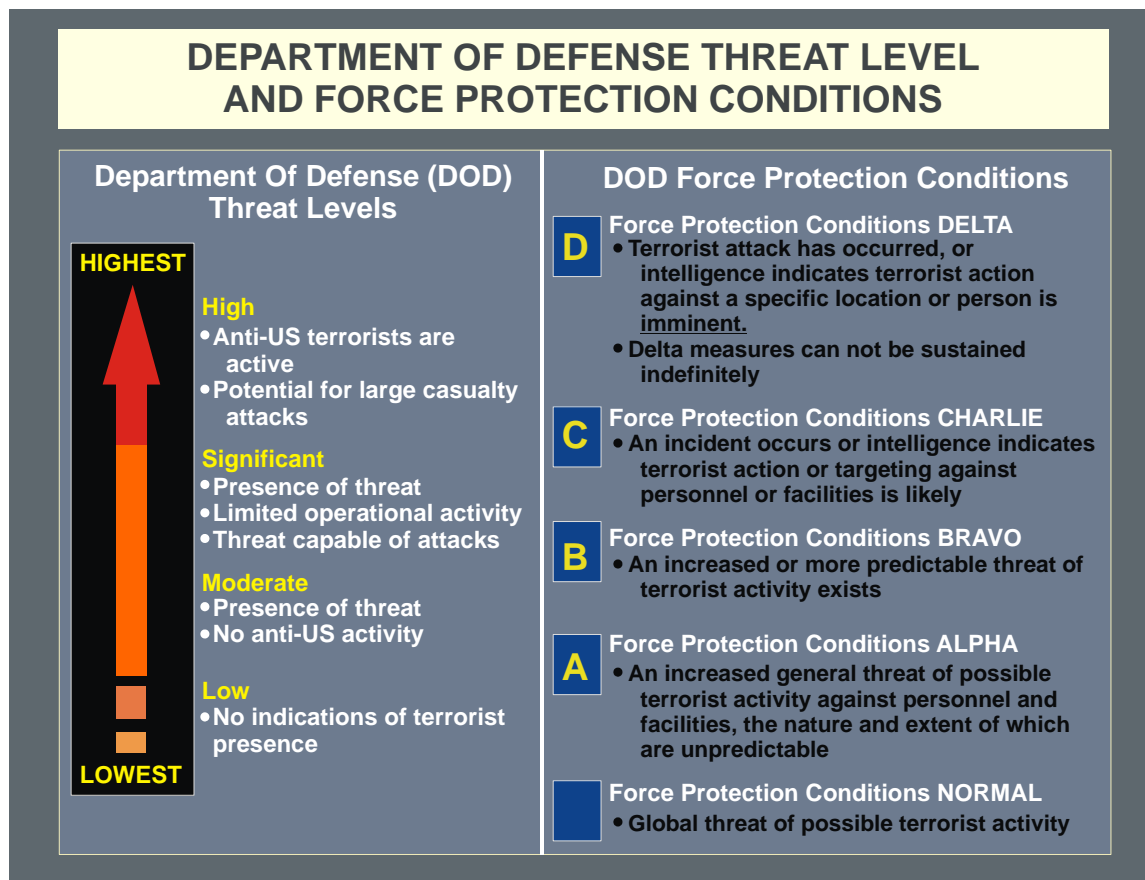


Figure V-1. Department of Defense Threat Level and Force Protection Conditions

g. **Program Review.** The program review evaluates the effectiveness and adequacy of the commander's AT program. The evaluation includes an assessment of the degree to which the program complies with the standards in DODI 2000.16, *DOD Antiterrorism (AT) Standards* and other higher HQ guidance. Additionally, the program review shall assess the risk management process implemented by the commander and the installation's ability to respond to a CBRN event. The AT program review can be conducted in conjunction with the local or higher HQ VA.

3. Countering Terrorist Attack Planning

Effective AT programs aim to detect, disrupt, and potentially defeat terrorist attack planning in order to ensure the safety of personnel and resources. To achieve this, AT plans should examine terrorist methods of surveillance, information gathering, and attack planning to determine the extent of training and resources needed to address the threat. In addition, AT plans must identify the most effective way to train personnel to counter terrorist attack planning with basic surveillance awareness procedures. This also requires identifying necessary surveillance detection requirements and promulgating incident reporting procedures. Most important, AT programs need to focus on building strong relationships with various LE and CI agencies. Indeed, this is a critical step in increasing the flow of information to neutralize the threat.

a. **Terrorist Methods of Surveillance and Information Gathering.** The typical terrorist attack planning process is best summarized in Figure V-2. Effective AT programs

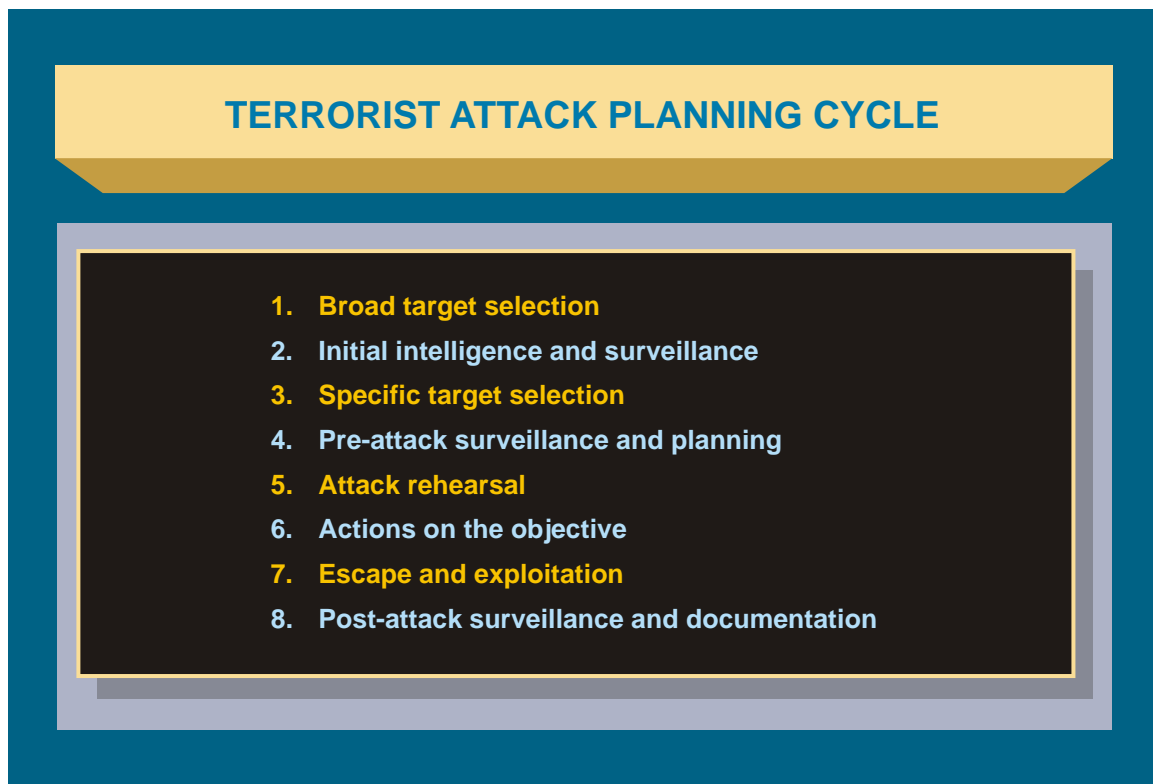


Figure V-2. Terrorist Attack Planning Cycle

aim to prevent or disrupt attacks by focusing on the initial stages in the terrorist attack planning process, where terrorists conduct initial surveillance and select targets for exploitation and suitability for attack. Terrorists examine security procedures, such as personnel and guard-force shift changes, access control procedures, frequency of roving security patrols, and the citizenship/nationalities of the guard forces. They also monitor installations or facilities to determine types of locks, access control devices, presence of closed-circuit security cameras, and the use of canine forces (military working dogs). Surveillance allows terrorists to assess gaps in physical security as well as identify patterns in standard operations procedures, including reaction times to emergencies, which can be used to plan for subsequent attacks against heavily fortified areas or emergency responders. When terrorists assess personnel in particular, they seek to identify vulnerabilities in human patterns such as modes and times of travel, frequently traveled routes, and the target's overall security awareness. Five techniques in the methodology that contributes to the terrorist attack planning cycle are *fixed (static) surveillance*, *mobile surveillance*, *technical surveillance*, *casual questioning (elicitation)*, and *probing*.

(1) **Fixed (Static) Surveillance.** 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 may attempt to establish observation posts near targets of interest in houses, apartments, offices, stores, restaurants, bars, bus stops, or on the street. A mobile surveillance platform, such as a parked car, truck, or recreational vehicle, can also serve as a semi-fixed observation post.

(2) **Mobile Surveillance.** Terrorists conduct mobile surveillance to follow targets. This can be done on foot (e.g., walking or jogging), in a vehicle, or a combination of the two. Mobile surveillance usually progresses from a fixed or static location to a vehicle follow, continuing until the target stops or arrives at its destination. At this point, terrorist operatives will position themselves to identify the target's departure. Meanwhile, other terrorist operatives will be positioned to cover the target's logical routes, thus enabling the surveillance to continue discretely after the target moves again. Terrorists can also follow targets using parallel routes, especially with a highly visible target such as a military convoy.

(3) **Technical Surveillance.** Terrorists may use a variety of electronic means to assist in surveillance, to include the use of recording devices (i.e. cell phone cameras and camcorders). Terrorists have also used the Internet to obtain private information, security information, and open-source Internet mapping data to assist in attack planning.

(4) **Casual Questioning (Elicitation).** Terrorist can acquire useful information on a target by simply asking questions. Through friendly, casual conversations terrorists are able to elicit security information, not necessarily from personnel willingly interested in divulging security procedures, but rather those that seem more approachable to the terrorist. Terrorists even exploit Internet chat rooms and other social networking media to acquire information needed for their attack planning.

(5) **Probing.** Terrorists may overtly approach secured areas carrying mock attack devices to determine firsthand the effectiveness of a facility's or installation's security

procedures and to gauge the vigilance and reaction of the security personnel. They may also conduct routine activities to desensitize security personnel or to produce false alarms to dull the effectiveness of security personnel. Examples of probing include:

- (a) Threats delivered via phone, email, or mail meant to elicit a security response.
- (b) Using some type of ruse to gain access or entry (e.g. approaching security checkpoints to ask for directions).
- (c) “Accidentally” attempting to smuggle contraband through checkpoints.
- (d) Leaving abandoned packages, vehicles, or other suspicious items near a target.
- (e) Noticeably watching and recording security reaction drills and procedures.

b. Surveillance Awareness. DOD personnel and their families must understand the implications of hostile surveillance; to assume that it is occurring, how to discretely detect or identify it, and what to do if they suspect it. In fact, personnel are often able to detect criminal or terrorist surveillance (i.e., targeting themselves or their installations) as a result of enhanced situational awareness orchestrated by aggressive AT programs. They may even make themselves less desirable targets by following the four fundamental principles of surveillance awareness: *stay informed, keep a low profile, be unpredictable, and stay alert*.

(1) **Stay informed.** This requires knowing the primary threats and terrorist elements operating in the immediate area. Commanders are responsible for keeping DOD personnel and their families informed of any changes in the local threat. More importantly, Service men and woman have a personal responsibility to increase their own situational awareness on the local threat and the operating environment. Certainly, it helps to know one’s neighbors (and their vehicles), the local vendors, and others who routinely operate near one’s home or place of work.

(2) **Keep a low profile.** Terrorists may find it harder to monitor someone who blends in with the local population. Low-key appearance and behavior may force terrorists to work harder to identify a target, either forcing them to get closer to their target or moving on to another one. As the terrorist gets closer, it also becomes *easier* for a potential target to detect the surveillance. To be sure, any effort by DOD personnel to aggressively elude or “ditch” the terrorist will only reduce the opportunity to detect the terrorist. Thus, one should maintain a normal demeanor and report what they see (see paragraph e, “Incident Reporting”).

(3) **Be unpredictable.** Through smart application of unpredictable behavior, routines, or travel, it is possible to greatly increase the time and resources required for terrorists to conduct surveillance. Deliberate variation of travel routes, for example, reduces the number of places a terrorist will select to plan an attack. This may frustrate them and force them to select more predictable locations or different targets. It is important, however,

to avoid selecting alternate travel routes that transit sparsely-populated, less-secure, or dense-traffic areas. In other words, do not change routes for the sake of changing routes.

(4) **Stay alert.** DOD personnel and their families need to know what to look for. Generally speaking, terrorists may look like they are trying to accomplish some “cover” task, but they will likely be paying more attention to their target, thus allowing themselves to be identified by an individual who has good situational awareness. Even more revealing is when a surveillance operative appears more than once in the vicinity of their target or behaves in a way that responds to what their target does. This is referred to as “correlation” and is considered one of the strongest indicators of hostile surveillance. (See Figure V -3 for a list of surveillance indicators).

c. **Surveillance Detection.** The fundamental principles of surveillance awareness discussed above (*stay informed, keep a low profile, be unpredictable, and stay alert*), if applied successfully, will directly contribute to detecting hostile surveillance by increasing the time, visibility, and efforts required to effectively target US personnel. *Surveillance detection* operations take it a step further by providing a commander the ability to move beyond ordinary FP measures and incident response to operations that will directly deter, detect, disrupt, and ultimately defeat the terrorist attack planning cycle. Simply stated, surveillance detection operations are used to detect and/or verify whether an individual, vehicle, or location is under surveillance. Surveillance detection teams, in particular, also identify specific locations where terrorists will most likely conduct surveillance or attack their targets, and then provide recommendations to a commander for resource application. Of note, surveillance detection should not be confused with countersurveillance operations which may involve more direct measures by trained security or intelligence professionals to counteract hostile surveillance, though surveillance detection and countersurveillance operations are often used in conjunction with each other (see JP 2-01.2, *Counterintelligence and Human Intelligence in Joint Operations*). The following are examples of what surveillance detection professionals can provide a commander:

(1) **Route Analysis for Key Personnel.** This involves noting areas along a travel route where terrorist are more likely to conduct surveillance, profile a potential target, or launch an attack. An example of this is areas where routes crisscross or overlap (including the beginning and end of a route which rarely changes), or where a route “channels” a target.

(2) **Likely Terrorist Attack or Surveillance Sites.** This entails determining the best locations for terrorist attacks and surveillance locations for profiling fixed or mobile targets. Potential surveillance and attack sites typically have the following characteristics: the site is routinely frequented by a mobile target at predictable times; has limited security or police presence; offers cover or camouflage for a hostile surveillance or attack team; offers a means to effectively control or limit the target’s movement to ensure success during the attack; and has a variety of good escape routes for the terrorist operatives.

(3) **Determining What Is Normal.** Knowing what is normal enables security personnel to detect deviations from routine activity, so that unusual or extraordinary behavior stands out. Surveillance detection teams can assist security personnel and military police in identifying anomalous activity.

SURVEILLANCE INDICATORS

1. Multiple sightings of the same suspicious person, vehicle, or activity, separated by time, distance, or direction
2. Correlation (over time, distance, and direction) that involves actions by persons that relate to the target (for example, when someone in the vicinity of a facility looks at his watch when key personnel enter or exit the main gate, or when guard shifts change)
3. Paying undue attention to a facility, person, vehicle, or area; drawing pictures, taking notes, or photographing security cameras or guard locations in areas not normally of interest to tourists
4. Measuring distances and counting steps
5. Electronic audio and video devices in unusual places
6. Extended loitering near potential targets
 - Sitting in a parked vehicle for an extended period of time
 - Long telephone conversations
 - Observing vehicles as they enter or leave a designated entry control point, facility, or parking areas
7. Out-of-place attire or behavior
 - Joggers resting or stretching for an unreasonable period of time
 - Not eating or leaving table before ordered food arrives
8. Nervous behavior
 - Staring or quickly looking away from individuals or vehicles
 - Fidgeting or appearing uneasy
 - Excessive perspiration

Figure V-3. Surveillance Indicators

Note: Skilled *surveillance detection* by ordinary DOD personnel involves formal training; however, the basic awareness techniques listed above should suffice for understanding suspicious behavior and evaluating daily routines. **It is important to emphasize that DOD personnel and their families should avoid confrontations with suspicious individuals whenever possible and allow security and LE professionals to take action.** It is never prudent to draw attention to oneself, or to try to outrun or aggressively avoid surveillance, unless there is a threat of injury or death.

d. **CI and LE Resources.** Regardless of the AT capabilities, resources, and protective measures in place, close working relationships with local, state, HN, and federal LE agencies are essential to establishing timely and effective responses to 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 the overall security of their units and the military community at large. If indicators continue despite well executed, overt security countermeasures and the trends clearly indicate preoperational terrorist attack planning, it may be necessary for commanders to implement more sophisticated, uniquely-tailored CI assets. See JP 2-01.2, *Counterintelligence and Human Intelligence in Joint Operations*.

e. **Incident Reporting.** Since terrorists frequently conduct extensive target surveillance—over a period of weeks, months, or years—their activities should be detectable. Moreover, terrorists will invariably commit mistakes, further increasing the chance of detection by ordinary individuals, security personnel, and trained surveillance detection teams. AT plans therefore require the most streamlined processes to expedite incident reporting of unusual activities so that information moves rapidly from the originator, through security and military police, and over to the required investigative and CI organizations. The best incident reports include detailed descriptions of the subject(s), time of day, locations, vehicles involved, and the circumstances of the sightings. Military police and security personnel need to report these incidents to their respective criminal investigative services or CI elements as soon as possible. Indeed, these incident reports are important pieces of information that, over time and in combination with other reported sightings (i.e., correlation of place, time, people, or method), allow investigators to accurately assess the threat.

Intentionally Blank

CHAPTER VI

TERRORIST INCIDENT RESPONSE

“One of the greatest dangers we continue to face is the toxic mix of rogue nations; terrorist groups; and nuclear, chemical, or biological weapons.”

Dr. Robert M. Gates
Secretary of Defense
27 January 2009

1. General

a. **Response to a Terrorist Incident.** The response to a terrorist incident includes procedures established to mitigate the effects of the incident. These procedures are designed to ensure the commander is able to rapidly deploy a terrorist incident response team to reduce further effects and damage; support emergency lifesaving and rescue functions; provide protection of DOD personnel and property; and, when appropriate, conduct or support criminal investigations. An important objective of AT incident response is to mitigate the number and severity of casualties resulting from a terrorist attack. Well-developed response measures can save lives, preserve health and safety, protect and secure property, and eliminate the hazard. A slow or uncoordinated response may result in additional loss of life, further damage to the installation, and the loss of public confidence in the organization’s ability to respond to a terrorist incident. Homeland Security Presidential Directive 5 mandates the use of the National Incident Management System (NIMS) using the Incident Command System (ICS) to facilitate a comprehensive and coordinated whole of government response at all levels.

b. **Planning Responsibility.** It is incumbent upon the commander to plan for, and be capable of reacting to, a terrorist attack using available assets until outside assistance arrives. DODI 2000.16, *DOD Antiterrorism (AT) Standards*, requires commanders to prepare installation-wide terrorist incident response measures and incorporate them into the AT plan. Terrorist incident response measures should include procedures for determining the nature and scope of incident response and procedures for coordinating security, fire, HAZMAT, and medical emergency responders. Most important, incident response measures must be fully coordinated, exercised, and evaluated. Although not direct elements of AT, plans for managing the consequences of a CBRN incident and continuity of essential military operations are important adjuncts to an effective AT program. Attacks employing CBRN weapons may produce massive casualties or widespread destruction, which can quickly overwhelm organic resources.

2. Incident Management Planning

a. At a minimum, AT plans should prepare for the most probable or likely threats as identified through the TA process and maximize the use of existing plans and SOPs. For instance, existing procedures for fire response, operation center management, disaster response, CBRN/HAZMAT response, security operations, and other related activities can be referenced in the document and do not need to be reproduced.

b. 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 comprise the emergency operations center (EOC) during an actual crisis. An effective method for determining what areas should comprise the planning and execution of the response is to use the emergency support functions as required by the National Response Framework (NRF). (See *National Response Framework* and DODI 6055.17, *DOD Installation Emergency Management Program*.)

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 the threat of violence. Detection may result from routine surveillance performed by an installation or facility intrusion-detection system, guard or security force, or in the case of bioterrorism, an unusual incidence of an infectious disease. Once detection of a terrorist act or incident has occurred, an initial assessment must be conducted by the first responding LE or security detachment.

b. Initial Response Force

(1) The initial response force is identified in the installation's/ship's terrorist response plans with on-scene command relationships and a clearly established chain of command. At facilities controlled by DOD agencies, the initial response force may be under the control of a senior civilian security official, DOD LE official, or senior fire official. When responding to requests for support from civil authorities, the initial response force acts in a supporting role to the civil authorities. However, the commander does not relinquish command responsibility and authority. 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 and all installations/ships must have trained personnel who are aware of the threat and are capable of reacting promptly 24 hours a day.

(3) Responses will vary according to the incident. For example, if terrorists escape before additional forces arrive, the initial response force should provide medical aid, seal off the 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 and interface with local LE or emergency service personnel, HN police, or military forces responding to the incident in accordance with existing MOAs and/or SOFAs.

c. Emergency Operations Center

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.

(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.

For additional information on EOC organization, see National Response Framework and DODI 6055.17, DOD Installation Emergency Management (IEM) Program.

(2) EOC emergency support function personnel should utilize available subject matter experts. For CBRN incidents, the DTRA operations center (OC) provides emergency responders and warfighters with continuous information on CBRN threats through on-line assistance, including hazard analysis and prediction modeling, and provides a wide-band infrastructure for user support. The DTRA OC can dispatch other DTRA resources as required. DTRA also provides AT program training via a mobile training team. The following Web sites are also sources of technical information useful for incident response planning: www.fped7.org; www.tswg.gov; and www.fema.gov.

d. **Confirmation.** Since the categorization of an incident will be a relevant factor in determining jurisdiction, 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. 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.

4. Initial Response to a Chemical, Biological, Radiological, or Nuclear Attack

a. Installations are required to establish an immediate response capability to ensure critical mission continuity and save lives during a CBRN 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 CBRN incident, the commander should direct the following complementary sets of actions:

(1) Activate mass notification advising 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 emergency responders have a plan and are equipped, trained, and exercised on the plan for responding to an incident involving CBRN.

d. Installations are required to include incident management measures in their AT plans. Use an effective and approved method for developing a comprehensive AT plan that systematically addresses the spectrum of response considerations. Nevertheless, terrorist CBRN incidents, or threats of terrorist CBRN acts, may overwhelm an installation's minimum capability to adequately detect, assess, or contain the threat. In the US, installation antiterrorism officers (ATOs) should consult with local fire and HAZMAT officials and the NRF available at the Federal Emergency Management Agency (FEMA) Web site to ensure complementary planning efforts.

See JP 3-41, Chemical, Biological, Radiological, or Nuclear Consequence Management, which provides joint doctrine for the military response to mitigate the effects of a chemical, biological, radiological, or nuclear event or incident, and DODI 2000.18, Department of Defense Installation Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive Response Guidelines, for equipment and training standards.

5. Special Considerations

a. **Establishing Communications.** A crucial aspect of implementing the AT plan is establishing communications among the forces in the incident area and the EOC. Communications personnel must be able to respond to changing needs during the incident and be able to maintain communications channels.

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, and other evidence, 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 or contamination of the scene can result in exclusion of the evidence. Indeed, all steps should be taken to allow qualified LE personnel to collect evidence. Types of evidence for which the chain must be established include:

- (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 staff judge advocate (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.

d. **Reports.** 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 reports are submitted to higher HQ 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) Disseminate information to inform people about the incident and support damage control/mitigation.
 - (b) Reiterate US policy on terrorism.

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

(2) DOJ has the lead PA responsibility for all 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 DOJ in providing specific PA support.

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

(4) DOS coordinates PA during terrorist incidents overseas. 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) PA representatives should be located in the EOC to keep abreast of incident activities. A media center should be located in a separate location away from the EOC. The public affairs officer (PAO) ensures that all information is released in accordance with established guidance and screened for intelligence information to maintain OPSEC. 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. Media representatives should be given access to all releasable information and to the scene as early as possible under reasonable conditions and restrictions commensurate with the risk and gravity of the event. Media can assist in disseminating information about the incident to inform and mitigate additional harm.

f. **Immediate Post-Incident Actions.** 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. 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. During the immediate post-incident phase, medical, psychological, and religious support, along with other support services, should be given to all personnel involved in the operation. Critical incident stress debriefing is a regular element of civilian emergency responder activities. Additional critical incident stress debriefing information is available at www.icisf.org. Contact the behavioral health office for additional Service guidance and support.

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 TTP. After action reports, whether for real incidents or exercises, are one mechanism for improving friendly capabilities and remaining ahead of the terrorist.

6. 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 its territories and possessions. For installations in the US, AT planning and response efforts (as it is for natural disaster and other hazards) will integrate NRF and NIMS principles as necessary because of the mutual interdependencies with local emergency management operations.

a. US National Incident Response

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

(2) The NRF establishes a comprehensive approach to enhance the ability of the US to manage domestic incidents. The plan incorporates best practices and procedures from incident management disciplines—HD, emergency management, LE, 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 USG coordinates with state, local, and tribal governments and the private sector during incidents. The NRF (available on the FEMA Web site) 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.

b. National Incident Management System. NIMS is a comprehensive national approach to incident management that is applicable at all jurisdictional levels and across functional disciplines.

(1) NIMS provides a consistent nationwide template to enable all government, private-sector, and NGOs 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. NIMS will enable responders at all levels to work together more effectively to manage domestic incidents no matter what the cause, size, or complexity. 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 NIMS include the following:

(a) Standardized organizational structures, processes, and procedures.

(b) Common 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 four 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. ICS is a proven on-scene, all-hazard incident management concept which is interdisciplinary and organizationally flexible enough to meet the needs of incidents of any size or level of complexity. ICS has been used for a wide range of incidents — from planned

events to HAZMAT spills to acts of terrorism and has become the standard for on-scene management.

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

(c) **Civil authority information support** is an authorized DOD capability for communicating information to domestic populations during national emergencies, such as terrorist incidents or natural disasters.

(d) **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 www.fema.gov/emergency/nims/.

Intentionally Blank

APPENDIX A ANTITERRORISM PLAN

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). If a more detailed plan is desired, the format for an OPLAN can be used, see Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3122.03C, *Joint Operation Planning and Execution System (JOPEs) Volume II, Planning Formats*. Inasmuch as this sample is for an AT plan some appendices to annexes will not line up with the format in JOPEs. However, annex titles have been kept consistent with JOPEs. Should a conflict exist between this appendix and the format found in CJCSM 3122.03C, the JOPEs manual takes precedence.

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 measures should be integrated into all plans.

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.

2. Sample Format

Note: All annexes referenced in the Sample Format below refer to annexes in JOPEs.

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 and key AT organization composition e.g., AT working group, crisis management team, EOC, first response elements. 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, MOUs/MOAs.)

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, CBRN 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 conventional and unconventional attack, including WMD.

(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 CBRN 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 CBRN 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 classified 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 set and maintained by DIA, 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 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.)

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 (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 CBRN 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 action 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 CBRN 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

(b) Task Listing

(2) Second Subordinate Unit/Element/Tenant

(a) Task Listing

(b) 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. Specific Annexes will provide amplifying instructions on these topics. The sections listed below are representative and may not be all-inclusive.

(1) AT Planning and Response. This template outlines AT planning and response elements on the installation required to respond to a terrorist/CBRN 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.

(2) Procedural

(a) Alert Notification Procedures. See Tab A (Counterterrorism) to Appendix 15 (Force Protection) to Annex C (Operations).

(b) Use of Force/Rules of Engagement. See Appendix 8 (Rules of Engagement) to Annex C (Operations).

(c) Installation Training and Exercises.

(d) Incident Response. See Annex T (Consequence Management).

(e) High-Risk Personnel Protection Procedures.

(f) AT Program Review.

(h) Higher Headquarters Vulnerability Assessments.

(3) Security Posture Responsibilities

(a) Law Enforcement.

(b) Physical Security to include Lighting, Barriers, Access Control. See Tab B (Physical Security) to Appendix 15 (Force Protection) to Annex C (Operations).

(c) Other On-site Security Elements.

(d) Operations Security. See Tab C (OPSEC) to Appendix 3 (Information Operations) to Annex C (Operations).

(e) Technology.

(f) EOC Operations.

(g) Critical Systems Continuity of Operations. See Appendix 16 (Critical Infrastructure Protection) to Annex C (Operations).

(4) Threat Specific Responsibilities

(a) Antiterrorism.

(b) Weapons of Mass Destruction. See Appendix 2 (CWMD) to Annex C (Operations).

(c) Special Threat Situations.

(d) Information Security. See Tab A (Information Security) to Appendix 1 (Information Protection) Annex K (Communications Systems Support).

(e) Natural/Man-Made Hazards (Optional).

(5) Special Security Areas

(a) Airfield Security. See Appendix 15 (Force Protection) to Annex C (Operations).

(b) Port Security. See Appendix 15 (Force Protection) to Annex C (Operations).

(c) Embarkation/Arrival Areas. See Appendix 15 (Force Protection) to Annex C (Operations).

(d) Buildings. See Appendix 15 (Force Protection) to Annex C (Operations).

4. ADMINISTRATION AND LOGISTICS. The administrative and logistics requirements need to support the AT plan. Ensure the staff conducts logistics planning for both pre- and post-incident measures addressing the following: locations of consolidated CBRN 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 CBRN defense equipment “push” packages. Specific logistics 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 E (Personnel).
- b. Logistics. See Annex D (Logistics).

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 CBRN 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 Systems Support).

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.)

Intentionally Blank

APPENDIX B

ANTITERRORISM CHECKLIST FOR COMMANDERS AND ANTITERRORISM OFFICERS

The following checklist is a self-assessment, management tool that can be used by commanders, agency managers, and unit antiterrorism officers to assess the status of their AT program.

Antiterrorism Checklist—Commanders
<p>Assuming Command:</p> <ul style="list-style-type: none"> • Does unit have an AT program and security posture appropriate for mission and potential threat? • AT officer appointed? • AT working group (ATWG) designated? • DIA and/or FBI threat assessment current? • Vulnerability assessment current? • AT plan complete? • Program review within past 12 months? • AT plan exercised within past 12 months? • AT level I training current? • Have you reviewed DODI 2000.16 and appropriate combatant commander/Service AT guidance? –Is combatant commander/Service AT guidance implemented?
<p>Organize for AT:</p> <ul style="list-style-type: none"> • Does unit have adequate focus on AT? • Is unit ATO school trained? • Are right functions represented in ATWG? • Is ATWG active? Meeting minutes? Accomplishments? • Next meeting? Next action?
<p>Threat Assessment:</p> <ul style="list-style-type: none"> • Do threat assessments provided by DIA and/or FBI and/or the local threat assessment process? <ul style="list-style-type: none"> • Identify specific terrorist capabilities, weapons, and tactics (to include CBRN). • Provide the necessary information for the commander to help tailor force protection conditions. • Have a review mechanism to provide up to date information. • Is unit aware of current and potential threats (conventional and CBRN)? • DIA and/or FBI (CONUS) assessed threat level for area? • Combatant commander-assigned higher local threat level? • Formal intelligence assessment on hand and current? • Relationship with supporting Intel activity? • Is counterintelligence or law enforcement support needed? • Local information considered? • Local information network established? • Aggressive list of threat options identified?
<p>Vulnerability Assessment (VA):</p> <ul style="list-style-type: none"> • Do vulnerability assessments and the vulnerability process include? • The range of terrorist threat identified in the threat assessment. • Recommendations for procedural enhancements and resource requirements. • Provided complete inventory of assets and areas. • Prioritization of assets/areas on criticality. • Catalog of known vulnerabilities. • Provide for annual revisions. • Has unit evaluated the vulnerability of all assets to potential threats to support risk management decisions? • When was the last vulnerability assessment? • Did last VA reveal significant vulnerabilities?

<ul style="list-style-type: none"> • What is status of remedial actions? • Next scheduled VA?
<p>Antiterrorism Plan:</p> <ul style="list-style-type: none"> • Does my unit have a suitable AT plan? • How is this plan documented? (Five par. order, or annexes to other orders?) • Does the plan specify the AT mission and concept of operation? • Does the plan lay out the task organization and mission essential or vulnerable areas (MEVAs)? • 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 plan provide actions at each FPCON? • Does plan provide a baseline for normal ops? • What FPCON measures have been adopted due to local threat? • Does plan provide diagram for random antiterrorism measures (RAMs)? • Does the plan include security force operations (including augmentation forces) and post priorities? • Has plan been reviewed within past year to remediate procedural and resource shortfalls? • Has plan been approved by higher HQ? • Received/approved AT plans from lower HQ? • Is the plan executable? • Is the plan resourced? • Does plan mitigate vulnerabilities with policy and procedural solutions? • Does plan address response to incident and mass casualties? • Does the AT plan contain, as a minimum, site specific procedures for? • Terrorism threat assessments. • AT physical security measures. • Mass notification procedures. • Incident response measures. • Measures to manage the consequences of AT incidents. • 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 and 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?
<p>AT Exercises:</p> <ul style="list-style-type: none"> • Has AT plan been validated by exercises and is unit ready to execute it? • Has AT plan been exercised within one year? • Have key organizations exercised their roles? • Unit response to increasing threat levels been exercised? • Unit response to incident/mass casualties been exercised? • AT plan been exercised in a manner to heighten awareness? Incorporated RAMs? • Has exercise identified discrepancies? Plan to correct them?
<p>Antiterrorism Resources:</p> <ul style="list-style-type: none"> • 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 headquarters? • Higher HQ approved these requirements? • Emergent and/or emergency needs submitted (e.g., Combatant Commander Initiative Fund [CCIF])? • Does the command incorporate AT requirements into the program change proposal process? • Are program change proposal requirements submitted for out year support of CCIF funded

<p>investments?</p> <ul style="list-style-type: none"> • Status of CCIF or program change proposal 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 (MILCON) standards? • Do structural engineers and security personnel work together to incorporate AT consideration in building design and review? • Are DOD AT Standards for buildings incorporated into new constructions? • How is technology being used to enhance security and human performance? • What technologies have been identified as recommended/required for higher threat levels/FPCONs? • Is the AT officer a member of the resource management committee?
<p>AT Training:</p> <ul style="list-style-type: none"> • Are personnel receiving the appropriate levels of AT training to include? <ul style="list-style-type: none"> • Level I-IV training. • High risk personnel. • AOR specific training prior to deployment. • A system to track and document training. • Is individual awareness of terrorism threat sufficient for threat environment/mission? • Annual level I training current? • AOR updates current and briefed? • Special local individual protective measures briefed and used?
<p>Program Review:</p> <ul style="list-style-type: none"> • Is AT program comprehensive, current, and effective? • Can unit do mission under FPCONs in use? • Are critical FPCONs compromised for unit morale or convenience? • Is AT a routine element of daily mission planning and execution? • Are operational patterns varied? • Is OPSEC included in mission planning? • Does unit continually monitor threat and corresponding security posture? • Does unit monitor and control access of visitors and employees in sensitive areas? • Has threat level changed since last VA? • Is threat assessment current and valid? • Are RAMs having desired effect on unit awareness, readiness, and deterrence?
<p>MOU/MOA:</p> <ul style="list-style-type: none"> • Is unit conforming to and employing MOU/MOA for local support? • Does unit or any detached personnel fall under the Department of State for force protection? • Are DOS's force protection instructions on hand for those individuals? • Identified organizations with jurisdiction for law enforcement, health, safety, and welfare of assigned service members on and off duty? • Unit conforming to jurisdictional agreements in these areas (SOFA, interagency)? • Identified local community organizations with shared security interests (police, federal law enforcement, hospitals, and public health)? • Mutual aid agreements in place with local community to leverage shared interests? • Mutual aid agreements been reviewed by higher HQ? • Mutual aid agreements executable (liability, jurisdiction, capabilities)?
<p>Mitigate WMD Effects:</p> <ul style="list-style-type: none"> • Has unit prepared for WMD attack? • Does AT plan consider terrorist use of WMD? • What are AT plan assumptions concerning the worst case threat options? • Procedures for detection of unconventional CBRN attacks? • Unit training include awareness of indicators of unconventional attacks? • Do all personnel have individual protective equipment available? • Are collective protective systems available? • What CBRN detection equipment is available? • What decontamination equipment is available? • Are decontamination procedures established?

<ul style="list-style-type: none"> • Are decontamination waste disposal procedures established in accordance with HN, federal, state, or local laws and regulations?
Off-Installation Housing: <ul style="list-style-type: none"> • Are personnel housed off-installation adequately secured? • 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)? • Incident response plans include measures for off-installation personnel (personnel warning system)?
Rules of Engagement (ROE)/Rules for the Use of Force (RUF): <ul style="list-style-type: none"> • Does unit have correct ROE/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 service members trained for making ROE/RUF decisions in realistic situations? • ROE/threat scenarios adequate and rigorous? • Is unit prepared to apply ROE/RUF for threat scenarios?

Questions for Facilities AT Officers

Antiterrorism Checklist—Antiterrorism Officers (ATOs)
DOD AT Policy: This standard does not apply.
Development of AT Standards <ul style="list-style-type: none"> • Do you have a copy of the applicable DOD, combatant commander, Service, and agency AT regulations, standards, and other guidance? • Combatant commander/Service and/or DOD agency standards should address: <ul style="list-style-type: none"> • Procedures to collect and analyze terrorist threat information, threat capabilities, and vulnerabilities to terrorist attacks. • Terrorism threat assessment, vulnerability assessment, terrorism incident response measures, and measures to manage the consequences of AT incidents. • AT plans and procedures to enhance AT protection. • Procedures to identify AT requirements and to program for resources necessary to meet security requirements. • DOD military AT constructions considerations.
Assignment of AT Operational Responsibility <ul style="list-style-type: none"> • Does the facility understand which combatant commander, Service or DOD agency has AT tactical control (TACON) for operational responsibility?
AT Coordination in Overseas Locations: This standard does not apply to facility AT plans.
Comprehensive AT Development, Implementation, and Assessment <p>Does the installation AT program contain, as a minimum, the following elements:</p> <ul style="list-style-type: none"> • Threat assessments • Planning • Exercises • Program review • Training • Vulnerability assessments
Antiterrorism Officers (ATOs) Assigned in Writing <ul style="list-style-type: none"> • Has the commander designated a Level II qualified/trained commissioned officer, non-commissioned officer, or civilian staff officer in writing as the ATO? • For deploying organizations (e.g. battalion, squadron, ship) have at least one Level II qualified individual designated in writing? • Has the ATO attended a Service approved Level II AT Training course?
Application of Department of Defense Terrorism Threat Analysis Methodology

<ul style="list-style-type: none"> • Does the unit use the DOD threat level methodology (Low, Moderate, Significant, High) in their local threat assessments?
Threat Information Collection and Analysis <ul style="list-style-type: none"> • Has the commander tasked the appropriate organization under their 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 warning reports and/or higher headquarters threat message?
Threat Information Flow <ul style="list-style-type: none"> • 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 between all organizations? • Does the command provide tailored threat information for transiting units?
Potential Threat of Terrorist Use of Weapons of Mass Destruction (WMD) <ul style="list-style-type: none"> • 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 AOR? • Is an estimate of terrorist potential use of WMD indicated in the local threat assessment?
Adjustment of Force Protection Conditions <ul style="list-style-type: none"> • Does the command have a process, based on terrorism threat information and/or guidance from higher headquarters, to raise or lower FPCONs?
FPCON Measures Implementation: This standard does not apply to facility AT plans.
FPCON Measures <ul style="list-style-type: none"> • Has the command developed site-specific measures or actions for each FPCON which supplement measures/actions enumerated for each FPCON? • Does the command have procedures to set and transition between FPCONs? • Does the command have procedures to establish a lower FPCON than Higher Headquarters? • Are site-specific AT measures, linked to FPCONs classified as a minimum, CONFIDENTIAL? • Site-specific AT measures separated from the AT plan can remain FOR OFFICIAL USE ONLY. • Do FPCONs permit sufficient time and space to determine hostile intent IAW standing ROE? • Has the command established procedures to expedite MOU/MOA assistance/response during elevated FPCONs?
Comprehensive AT plan <ul style="list-style-type: none"> • Does the command have a signed AT plan? • Is the plan site-specific and address the following key elements? • Terrorism threat assessment (including WMD). • Vulnerability assessment. • Risk assessment. • AT physical security measures. • Terrorism incident response measures. • Measures to manage the consequences of AT incidents. • Does the installation incorporate AT planning into operations orders for temporary operations or exercises?
Terrorism Threat Assessment <ul style="list-style-type: none"> • Does the command have an annually updated terrorism threat assessment? • Does the threat assessment consider the following during the assessment process: <ul style="list-style-type: none"> • Capabilities of the terrorist threat. • Vulnerability of the facilities. • Criticality of the facilities. • Is the threat assessment used as the basis and justification for recommendations on AT enhancements, program/budget requests and establishment of FPCONs? • Does the command use a risk assessment to integrate threat and vulnerability assessment information in order to make an informed decision to commit resources and/or enact policies and procedures to mitigate the threat or define the risk?

<ul style="list-style-type: none"> • Does the risk assessment analyze the following elements? <ul style="list-style-type: none"> • Terrorist threat. • Criticality of the assets. • Vulnerability of facilities, programs, and systems to terrorist threats. • The ability to conduct activities to deter terrorist incidents, employ countermeasures, mitigate the effects of a terrorist incident, and recover from a terrorist incident.
<p>AT Physical Security Measures</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Physical structures. • Physical security equipment. • CBRN 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?
<p>Terrorist Incident Response Measures (first response)</p> <ul style="list-style-type: none"> • Has the command prepared installation-wide and/or shipboard terrorist incident response measures which include: <ul style="list-style-type: none"> • 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?
<p>Manage the Consequences of AT Incidents</p> <ul style="list-style-type: none"> • Do measures 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 host nation support? • Do measures include guidelines for predeployment and garrison operations, pre-attack procedures, actions during attack, and post-attack actions?
<p>Training and Exercises</p> <ul style="list-style-type: none"> • Has the command conducted field and staff training (annually) to exercise AT plans to include? <ul style="list-style-type: none"> • AT physical security measures. • Terrorist incident response measures. • Measures to manage the consequences of AT incidents. • Does the command maintain exercise after action reports (AARs)/lessons learned and document actions taken to remediate identified shortfalls for at least a year? • Does command predeployment training include training and exercises? <ul style="list-style-type: none"> • Credible deterrence/response. • Deterrence-specific tactics, techniques, and procedures. • Terrorist scenarios and hostile intent decision making.
<p>Comprehensive AT Review</p> <ul style="list-style-type: none"> • Does the command review own and subordinate AT programs and plans at least annually to facilitate AT program enhancement? • Does the command review the AT program when the terrorist threat level changes?
<p>General Requirements for AT Training</p> <ul style="list-style-type: none"> • Does the command ensure all personnel records are updated to reflect AT training IAW DOD component policy?
<p>Level I AT Awareness Training</p> <ul style="list-style-type: none"> • Does the command conduct Level I training IAW DOD and combatant commander/Service/agency

standards? <ul style="list-style-type: none"> • Does the installation ensure Service family members traveling beyond CONUS on official business receive Level I training (i.e., PCS move)?
AOR-Specific Training Requirements for all Department of Defense Personnel <ul style="list-style-type: none"> • Does the command ensure all individuals traveling outside CONUS for either permanent or temporary duty complete Level I AT awareness training? • Has the command provided combatant commander approved AOR specific AT protection information to individuals traveling outside CONUS within three months prior to travel? • Does the command ensure intra-theater transiting units receive detailed threat information covering travel routes and sites that will be visited by the unit?
Level II Antiterrorism Officer (ATO) Training <ul style="list-style-type: none"> • Does the installation and/or each deployed unit have at least one Level II trained ATO assigned? • Have 0-5/0-6 commanders received Level III training prior to assumption of command?
Training for High-Risk Personnel and High-Risk Billets <ul style="list-style-type: none"> • 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?
Vulnerability Assessments of Installations <ul style="list-style-type: none"> • Has a local vulnerability assessment been conducted within the past year? • Did the vulnerability assessment identify vulnerabilities and means to eliminate or mitigation them? • Did the vulnerability assessment identify options for enhanced protection of DOD personnel and assets? • Does the AT vulnerability assessment assess the following functional areas at a minimum: <ul style="list-style-type: none"> • AT plans and programs. • Counterintelligence, law enforcement, liaison, and intelligence support. • AT physical security measures. • Vulnerability to a threat and terrorist incident response measures. • Vulnerability assessment for terrorist use of WMD. • 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, local community, and where appropriate, inter-Service and tenant organizations to enhance force protection measures or respond to a terrorist incident. • Status of formal and informal agreements to support AT functions. • Does the vulnerability assessment 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?
Predeployment AT Vulnerability Assessment <ul style="list-style-type: none"> • Has a predeployment AT vulnerability assessment been conducted for units prior to deployment? • Have appropriate AT measures been implemented to reduce risk and vulnerability? • Has the command received onboard and/or advance-site assessments prior to and during visits to higher-threat areas of significant or high threat Levels or where a geographically specific terrorism threat warning report is in effect? • Has the command requested funds from CCIF for emergent AT requirements prior to movement of forces? • Has the command explored the use of commercial-off-the-shelf or government-off-the-shelf products to meet near-term AT protection requirements?
Construction Considerations <ul style="list-style-type: none"> • Do DOD components adopt and adhere to common criteria and minimum construction (i.e., new construction, renovation, or rehabilitation) standards to mitigate AT vulnerabilities and terrorist attacks?
Facility and Site Evaluation and/or Selection Criteria <ul style="list-style-type: none"> • 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.

<ul style="list-style-type: none"> • Has the command used these factors to determine if facilities can adequately protect occupants against terrorism attack?
<p>AT Guidance for Off-Installation Housing</p> <ul style="list-style-type: none"> • 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 permanently 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 appropriate, 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: <ul style="list-style-type: none"> • Facilities used by DOD employees and their dependents. • Transportation services and routes used by DOD employees and their dependents.
<p>Executive Protection and High Risk Personnel Security</p> <ul style="list-style-type: none"> • 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?
<p>Miscellaneous Issues</p> <ul style="list-style-type: none"> • Does the command have technology to access critical terrorism intelligence e.g., SIPRNET? • Has the 0-6 through 0-8 commander been to Level IV training?

APPENDIX C

THREAT INFORMATION ORGANIZATION MATRIX

1. Introduction

The following matrix (see Figure C-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. DOD intelligence oversight regulations and guidance remain in effect for all CONUS collection, analysis, and reporting on terrorist threats or suspicious activities. Similarly, AT threat analysis and reporting shall be conducted in accordance with the same intelligence oversight guidance.

INSTALLATION THREAT INFORMATION ORGANIZATION PLAN																			
PIR	IR	Indicators	Specific Information Requirements	Collection		Collection Agencies													
				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	SI LEA	DOJ/MT
																			Near Base
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
	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
		1.11. Information on purchase or theft of material to make improvised devices	1.11a. Report unusual purchase or theft of explosives, weapons, ammunition, HAZMAT, fertilizers, chemicals, etc.	Always	Never														
		1.12. Information on purchase of large quantity of weapons or theft of weapons	1.12a. Report unusual purchase or theft of vehicles capable of being configured with explosives or WMD	Always	Never														
		1.13. Information on suspicious car, truck, van activity	1.13a. Report 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 theft of government vehicles or license plates	Always	Never														
			1.14b. Report purchase or theft of vehicles with DOD decals																
			1.14c. Report loss or theft of military IDs or special access passes																

Figure C-1. Installation Threat Information Organization Plan

INSTALLATION THREAT INFORMATION ORGANIZATION PLAN																	
PIR	IR	Indicators	Specific Information Requirements	Collection		Collection Agencies											
				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
PIR #1	Installation																
		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 or access XXXX computer network	1.16a. Report any attempt to access XXXX computer network or reports of stolen or misused passwords														
			1.16b. Report any ADP viruses immediately														
			1.16c. Report any suspicious telephone calls or e-mails.														
	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 increased 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 with 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 or detained vicinity XXXX														

Figure C-1. Installation Threat Information Organization Plan (cont.)

INSTALLATION THREAT INFORMATION ORGANIZATION PLAN																				
				Collection		Collection Agencies														
				Date Info Needed	Date Info No Longer Needed	CID, OSI, NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Loc LEA #1	Loc LEA #2	Loc LEA #3	SI LEA	DOMINT	I	Near Base
PIR	IR	Indicators	Specific Information Requirements			LET														Remarks
PIR #1	Installation			Always	Never															
	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 e-mails	Always	Never															
		1.34. Requests for information on XXXX activities, missions, memoranda of agreement, memoranda of understanding	1.34a. Report all questions about sensitive locations																	
		1.35. Active dissident or terrorist groups recruiting vicinity XXXX	1.35a. Report all questions about working relationships with local, state, federal law enforcement agencies																	
		1.36. Active dissident or terrorist groups fund-raising vicinity XXXX	1.36a. Report all suspicious requests for job employment vicinity XXXX																	
		1.37. Active dissident or terrorist groups training vicinity XXX	1.37a. Report all suspicious fund-raising operations vicinity XXXX																	
			1.37b. Report all suspicious recruiting or training operations vicinity XXXX																	
			1.37c. Report what these groups collect against																	
		1.38. Recent arrests in vicinity XXXX	1.38a. Report any suspicious individuals arrested or detained vicinity XXXX																	

Figure C-1. Installation Threat Information Organization Plan (cont.)

INSTALLATION THREAT INFORMATION ORGANIZATION PLAN																			
PIR	IR	Indicators	Specific Information Requirements	Collection		Collection Agencies													
				Date Info Needed	Date Info No Longer Needed	LET	CID, OSI, NCIS	CI	TWG	HHO INT	CST	HS	FBI	ATF	Loc LEA #1	Loc LEA #2	Loc LEA #3	SI LEA	DOJ/MT
PIR #1	Installation																		
	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 or terrorist organizations are using to obtain information, surveil, recruit, fund-raise, or acquire weapons or 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 e-mails	Always	Never														
		1.44. Queries about XXXX security measures	1.44a. Report all suspicious requests for job employment in vicinity XXXX																
			1.44b. Report all suspicious recruiting or training operations vicinity XXXX																
PIR #2	Installation																		
	2. What patterns of activity, threats, or law enforcement advisories have there been that indicate an increased likelihood of attack on XXXX or the surrounding community?																		

Figure C-1. Installation Threat Information Organization Plan (cont.)

INSTALLATION THREAT INFORMATION ORGANIZATION PLAN																
PIR	IR	Indicators	Specific Information Requirements	Collection		Collection Agencies										
				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
PIR #2	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 individuals videotaping, photographing, or sketching installation elements													
		2.12. Incidents of unauthorized individuals attempting to access XXXX	2.12a. Report turnarounds at gates													
			2.12b. Report loss or theft of military IDs or special access passes													
		2.13. Incidents of XXXX personnel being surveilled by suspicious personnel	2.13a. Report any suspicious incidents in which 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 or unusual circumstances involving the loss of personal ID cards, vehicle registrations, government license plates, or government vehicles?															
		2.21. Incidents of stolen or lost personal ID cards	2.21a. Report loss or theft of government vehicles or license plates													

Figure C-1. Installation Threat Information Organization Plan (cont.)

INSTALLATION THREAT INFORMATION ORGANIZATION PLAN																
PIR	IR	Indicators	Specific Information Requirements	Collection		Collection Agencies										
				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
PIR #2	Installation															
		2.22. Incidents of stolen or lost DOD decals or special access passes for XXXX	2.22a. Report purchase or theft of vehicles with DOD decals													
		2.23. Incidents of stolen or lost government license plates	2.23a. Report loss or 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													
		2.26. Queries of unauthorized personnel attempting to obtain XXXX access passes	2.26a. Report all suspicious requests for employment in vicinity XXXX													
	2.3. Have there been thefts or unusual circumstances involving the loss of personal or government weapons, ammunition, or explosives?															
		2.31. Increased reporting of theft of weapons, ammunition, or explosive materials in vicinity XXXX	2.31a. Report unusual purchase or theft of explosives, weapons, ammunition, HAZMAT, fertilizers, chemicals, etc.													
		2.32. Attempts to illegally purchase weapons, ammunition, or explosive materials	2.32a. Report unusual purchase or theft of vehicles capable of being configured with explosives													
		2.33. Unusual queries about location of storage of weapons on XXXX, especially by telephone or e-mail	2.33a. Report on vehicles modified to handle heavier loads													

Figure C-1. Installation Threat Information Organization Plan (cont.)

INSTALLATION THREAT INFORMATION ORGANIZATION PLAN																
PIR	IR	Indicators	Specific Information Requirements	Collection		Collection Agencies										
				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
PIR #2	Installation															
		2.34. Attempts by unauthorized individuals to observe military training sites where weapons are used	2.34a. Report loss or theft of government vehicles or license plates													
	2.4. Have there been any perimeter violations, security breaches, unauthorized intrusions, or unauthorized overflights of XXXX?															
		2.41. Incidents of physical signs of intrusion on XXXX	2.41a. Report loss or theft of government vehicles or license plates													
		2.42. Incidents of unauthorized personnel attempting to access XXXX	2.42a. Report on purchase or theft of vehicles with DOD decals													
		2.43. Incidents of unauthorized attempts to access XXXX	2.43a. Report loss or theft of military IDs or special access passes, refused entries, or turnarounds at gate													
	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 nationwide	2.51a. Report any suspicious mail, packages, or cargo received on/vicinity XXXX													

Figure C-1. Installation Threat Information Organization Plan (cont.)

[illegible]

INSTALLATION THREAT INFORMATION ORGANIZATION PLAN																					
				Collection		Collection Agencies															
				Date Info Needed	Date Info No Longer Needed	LET	CID, OSI, NCIS	CI	TWIG	HHQ INT	CST	HS	FBI	ATF	Loc LEA #1	Loc LEA #2	Loc LEA #3	SI LEA	DOM/IT	Near Base I	
PIR	IR	Indicators	Specific Information Requirements																		Remarks
PIR #2	Installation																				
		2.64. Incidents of suspicious individuals trying to gain employment at businesses that have access to aircraft, commercial vehicles, tanker trucks, watercraft	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 opportunity for threat or 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?																				
		3.11. Unusual number of queries concerning events taking place on/vicinity XXXX	3.11a. Report any unusual questions about events taking place on/vicinity XXXX																		
		3.12. Increased number of reports nationally about threat to major sporting, cultural, industrial, political, military, or other symbolic events	3.12a. Report increase in threat reporting nationwide concerning major sporting, cultural, industrial, political, military, or symbolic events																		
		3.13. Incidents of unauthorized individuals attempting to gain access to events on/vicinity XXXX	3.13a. Report all suspicious questions about XXXX or vicinity																		

Figure C-1. Installation Threat Information Organization Plan (cont.)

INSTALLATION THREAT INFORMATION ORGANIZATION PLAN																			
PIR	IR	Indicators	Specific Information Requirements	Collection		Collection Agencies													
				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	SILEA	DOJ/MT
PIR #3	Installation																		Near Base
		3.14. Incidents of individuals making queries about security measures pertaining to events on/vicinity XXXX	3.14a. Report all suspicious telephone calls or e-mails																
		3.15. Incidents of suspicious individuals attempting to gain employment to support specific events on/vicinity XXXX	3.15a. Report suspicious attempts to gain employment at special events																
	3.2. What movements of HAZMAT take place on XXXX or in 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 HAZMAT on/vicinity XXXX	3.21a. Report unusual queries concerning movement of HAZMAT from XXXX																
		3.22. Incidents of suspicious individuals trying to gain employment at businesses that have access to HAZMAT	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 HAZMAT	3.23a. Report thefts or individuals making queries about security measures pertaining to movement of HAZMAT on/vicinity XXXX																
		3.24. Increased number of reports nationally about threat surrounding use of HAZMAT	3.24a. Report news concerning threat surrounding use of HAZMAT																

Figure C-1. Installation Threat Information Organization Plan (cont.)

INSTALLATION THREAT INFORMATION ORGANIZATION PLAN																				
				Collection		Collection Agencies														
PIR	IR	Indicators	Specific Information Requirements	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	SI LEA	DOM/IT	Near Base
PIR #4	Installation																			Remarks
4. Do indicators exist of a possible incident at XXXX or the surrounding community involving nuclear, biological, or chemical weapons?																				
	4.1. Do threat organizations have the means to conduct a CBRN attack or a HAZMAT attack at XXXX or in the surrounding community?																			
		4.11. Incidents of stolen CBRN material nationally and specifically in vicinity XXXX	4.11a. Report stolen CBRN material in vicinity XXXX																	
		4.12. Incidents of unusual purchase of explosives, weapons, ammunition, HAZMAT, fertilizers, chemicals, precursors, etc.	4.12a. Report excessive or unusual purchases of potential CBRN material																	
		4.13. Incidents of unusual purchase or theft of vehicles capable of being configured with explosives or 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 CBRN-related measures on/vicinity XXXX	4.14a. Report suspicious queries about the capability of CBRN materials																	
		4.15. Incidents of individuals making queries about security measures pertaining to CBRN-related measures on/vicinity XXXX	4.15a. Report queries about the security of chemicals used to train on XXXX																	

Figure C-1. Installation Threat Information Organization Plan (cont.)

INSTALLATION THREAT INFORMATION ORGANIZATION PLAN																						
				Collection		Collection Agencies																
				Date Info Needed	Date Info No Longer Needed																	
PIR	IR	Indicators	Specific Information Requirements			CID, OSI, NCIS LET	CI	TWIG	HHQ INT	CST	HS	FBI	ATF	Loc LEA #1	Loc LEA #2	Loc LEA #3	SI LEA	DOM/IT	I	Near Base	Remarks	
PIR #4	Installation																					
		4.16. Increased reporting of terrorist organization's ability and threat to CBRN material in the US	4.16a. Report unauthorized individuals attempting to gain access to XXXX																			
		4.17. Treatment of 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 antidotes																			
			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 or plant life																			
	4.2. Do these threat organizations have a history of conducting CBRN attacks?																					
		4.22. Past reporting of a terrorist group in vicinity XXXX utilizing CBRN material to conduct attacks	4.22a. Review records and report previous CBRN activity of local domestic dissident groups																			
	4.3. What indicators suggest that a threat organization is about to conduct an attack?																					
		4.31. Incidents of threats to conduct CBRN attacks in vicinity XXXX	4.31a. Report all related threats																			
		4.32. Incidents of stolen CBRN materials in vicinity XXXX	4.32a. Report all stolen chemical agents																			
		4.33. Incidents of queries about XXXX's ability to respond to a CBRN attack	4.33a. Report all suspicious inquiries about CBRN defense capabilities																			

Figure C-1. Installation Threat Information Organization Plan (cont.)

INSTALLATION THREAT INFORMATION ORGANIZATION PLAN																			
PIR	IR	Indicators	Specific Information Requirements	Collection		Collection Agencies													Remarks
				Date Info Needed	Date Info No Longer Needed	CID, OSI, NCIS	CI	TWG	HHQ INT	CST	HS	FBI	ATF	Loc LEA #1	Loc LEA #2	Loc LEA #3	SILEA	DOIM/IT	
PIR #4	Installation																		
		4.34. Incidents of unusual purchases of CBRN protective gear	4.34a. Report thefts or purchases of CBRN protective gear																
	4.4. Where are HAZMAT stored, transported, or used in bulk on XXXX or in the surrounding community, which could create mass casualties?																		
		4.41. Chemical or manufacturing 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 these facilities store, receive, or ship chemicals																
			4.41d. Report suspicious incidents related to storage or shipment of chemicals																

Legend

ADP automated data processing
 ATF Alcohol, Tobacco, and Firearms
 CBRN chemical, biological, radiological, and nuclear
 CI counterintelligence
 CID Criminal Intelligence Division
 CST civil support team
 DOD Department of Defense
 DOIM/IT Department of Information Management/Information Technology
 FBI Federal Bureau of Investigation
 HAZMAT hazardous materials
 HHQ INT higher headquarters intelligence
 HS homeland security
 I installation

ID identification
 IR information requirement
 LEA law enforcement agency
 LET law enforcement team
 Loc local
 MI military intelligence
 NCIS Naval Criminal Investigation Service
 OSI Office of Special Investigations
 PIR priority information requirement
 St state
 TWG threat working group
 WMD weapons of mass destruction

Figure C-1. Installation Threat Information Organization Plan (cont.)

APPENDIX D

PREVENTIVE MEASURES AND CONSIDERATIONS

1. Commander's Responsibility to Manage the Risk of Terrorism

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, rotation, 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. 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* and UFC 4-020-01, *DOD Security Engineering Facilities Planning Manual* contains a flow chart and other information to support development of a DBT for facility planners.

b. The DBT is used by engineering and facilities personnel to protect personnel and mission infrastructure 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. The DBT is also used by security personnel manning entry control points to develop search procedures to prevent the on-base DBT from being exceeded.

c. Installations can determine the DBT by identifying the highest threat severity and tactic that they will likely face. The threat working group can develop a threat matrix from the analysis of the threat assessment. The threat matrix, when properly completed, will identify the installation's DBT for all identified threats and hazards. Additionally, the combatant command's enhanced threats and hazards assessment for the Defense Critical Infrastructure Program can assist in developing the DBT from an all-hazards perspective. The installation commander must at a minimum, implement the higher headquarters directed

DBT. If higher HQ guidance does not provide a DBT, the installation should establish and incorporate a DBT for use by security engineers and security forces.

d. The generic design threat of a bomb (equivalent explosive weight in TNT [Trinitrotoluene]) placed in a stationary vehicle inside the installation perimeter drives facility standoff. Determining the minimum standoff from parking and roadways at mission essential vulnerable areas (MEVAs), 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. Similar design threat input is needed in the AT plan for moving vehicle attack and ballistics attack. Where the DBT includes the threat from a moving vehicle, a barrier plan incorporating sufficient counter-mobility features to prevent a vehicle from intruding into the standoff area is required. 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 to facilities along and outside the controlled perimeter is different from the threat posed to facilities inside a controlled perimeter. Whenever possible, commanders should adopt the off-base DBT in the design of protective systems for existing facilities and in the construction or renovation of new facilities if these facilities are vulnerable to off-base threats. Of note, the on-base DBT needs to take into consideration the ability to mitigate threats at access control point and circumstances where on-base facilities are located close enough to off-base areas where vehicles may be located (e.g., off-base parking lot next to the perimeter).

3. Joint Security Areas

During joint and multinational operations, US units and bases in the joint security area (JSA) 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 JSA are still required to maintain AT measures commensurate with the JSC's guidance. Specific TTP for operations in the JSA are contained in JP 3-10, *Joint Security Operations in Theater*.

4. Preventive Measures

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 nonlethal means such as vehicle light arresting device, portable vehicle arresting barrier, spike strips, caltrops, dragon teeth, or tire shredders to slow down unauthorized traffic. 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.

b. **Entry Control Points (ECPs).** ECP design 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. ECP design should also attempt to maximize response time by determining identity of threats as early as possible and minimize risk to personnel seeking entrance to the installation.

c. **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 and technologies, including nonlethal weapons, for responding to terrorist attacks and during escalation of force incidents. 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.

5. 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, and the installation of remotely operated long range persistent sensors systems such as electro optical/infrared, seismic acoustic – thermal imaging technologies.

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.

f. **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 which includes all available weapons for escalation of force.
- (5) Employment of non lethal weapons to address escalation of force incidents.
- (6) Key words, e.g., words to use under duress.
- (7) Response to unauthorized photography and surveillance activities. Identification of probable threat surveillance locations and response to unauthorized photography and surveillance activities.
- (8) Steps necessary to obtain police, reaction force(s), fire department, and ambulance.
- (9) Guidelines for contact with HN police.
- (10) Guidelines for contact with press and media.
- (11) Evacuation procedures.

6. Antiterrorism While in Transit

a. **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) Confirm that drivers have received appropriate antiterrorism training for the vehicles and conditions in which they will be operating.
- (2) Avoid establishing a regular pattern.
- (3) Vary routes and timing.
- (4) Travel in groups, never single vehicles.
- (5) Do not stop for dead or dying animals in/beside the road.
- (6) Do not allow people to walk up to vehicles.

(7) 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).

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

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

(10) Plan communications requirements.

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

(12) Provide adequate security.

(13) Plan in advance for maintenance and evacuation.

(14) Use surveillance detection or countersurveillance.

(15) Use counter radio-controlled IED electronic warfare systems.

b. 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.

c. **Convoys.** In extremely high-risk areas, convoy protection mission planning should include the employment of armed escorts equipped with both lethal and nonlethal weapons capabilities.

(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 and location. 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. Aircraft, including helicopters, attack and close air-support, and unmanned aerial vehicles (UAVs), 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 operations.

(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.

For additional information on convoy operations, refer to Field Manual 4-01.45/Marine Corps Reference Publication 4-11.3H/Navy Tactics, Techniques, and Procedures P 4-01.3/Air Force Tactics, Techniques, and Procedures 3-2.58, Multi-Service Tactics, Techniques, and Procedures for Tactical Convoy Operations.

d. **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 USG 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, UAV).
- (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).

e. **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 or congested waterways such as straits, harbors, or anchored off hostile coastlines are visible and high-risk targets. Crews of ships need to evaluate each new port and determine possible terrorist actions and ship's force counteractions (such as using fire and steam hoses and other nonlethal weapons to repel or deter 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 weapon (including nonlethal 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.

f. **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.

g. **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 SJA office and be in accordance with any applicable basing, status-of-forces, or other agreements. Depending on applicable agreements and regulations or other policy, patrols may be authorized to support police operations, expand the area of influence, gather information, police nightclubs and restaurants, detain individuals as required, conduct hasty 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.

h. **Roadblocks.** There are two types of checkpoints: deliberate and hasty. Deliberate checkpoints are permanent or semi-permanent roadblocks/control points 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 effectiveness 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. Checkpoints 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.

i. **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.

j. **Guardian Angel/Protective Over Watch.** The Guardian Angel/protective over watch construct is a force protection measure for active observation, early threat warning, and, when required, engagement. As an element of force protection planning it may apply in any environment. Essential elements include distinct ROE/RUF, communications with adjacent and supporting security and reaction forces, and decentralized decision-making authority to allow for rapid decision making, based on extant conditions.

k. **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.

l. **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 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.

m. **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.

APPENDIX E

RISK MANAGEMENT PROCESS

The risk management process is the foundation of any AT program. It incorporates **CAs, VAs, and TAs** into a target-specific **RA**. Methodologies used to determine levels of threat, criticality, vulnerability and risk are explained in detail below.

1. Criticality Assessment

Criticality of an asset is determined by the importance that its incapacitation or destruction would have on mission-essential operations. Critical assets can be people, physical entities, or information. They can be located either within or outside the US and employed, owned, or operated by domestic, foreign, public, or private sector organizations. Both regulations and the commander's priorities and intent determine critical assets. Regulations cover items such as HRP, ammunition storage areas, etc. The commander's intent extends coverage to other items such as mission critical and high occupancy assets.

a. Conducting the Criticality Assessment

(1) The CA identifies assets supporting DOD missions, units, or activities which are 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.

(2) 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 to determine:

- (a) **Key assets** of the installation/unit.
- (b) **Critical functions** and the extent they can be replicated under various attack scenarios.
- (c) **Time required** to duplicate key assets or infrastructures efforts if temporarily or permanently lost.
- (d) **Priority of response** to key assets, functions, and infrastructures in the event of fire, multiple bombings, or other terrorist acts.

(3) 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, both have design limitations and are best used only as an adjunct to the risk management process. DOD Manual 3020.45-V1, *Defense Critical Infrastructure Program (DCIP) (DOD Mission-Based Critical Asset Identification Process [CAIP])*, provides comprehensive procedures for a defense critical infrastructure identification process using a mission-focused process.

(4) The purpose of the criticality assessment process is to identify, classify, and prioritize all assets on an installation. Assets can include personnel, equipment, stockpiles, buildings, or transportation systems that are deemed critical as defined by DODD 3020.40, *Defense Critical Infrastructure Program*. Assets can be classified as MEVAs, high risk targets, HRP, higher headquarters, incident response and recovery, supporting foundational infrastructure networks, high demand, and low density. 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.

For more information on high risk billets and HRP, see DODI O-2000.22, Designation and Physical Protection of DOD High Risk Personnel (HRP).

(5) 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.

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

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

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

(c) **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.

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

(e) **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 and in a timely fashion?

(f) **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?

b. Other Methodologies: MSHARPP and CARVER

(1) 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, while CARVER is not specifically tailored for AT assessments, it can be adapted. 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.

(2) MSHARPP

(a) 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 effects on community) of potential targets. This section provides an example of how to use MSHARPP.

(b) 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.

(c) **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.

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

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

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

c. **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.

2. **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.

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

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

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

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

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

(d) **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:

1. ONE. Low profile or obscure symbol, demonstrates no strength or capability not common knowledge.

2. TWO. Low profile, direct symbol, local publicity, demonstrates no new capability or willingness.

3. THREE. Symbolic, achieves limited global publicity, demonstrates no new capability or willingness.

4. FOUR. Prominent symbol, global publicity, demonstrates previously unconfirmed capability or willingness.

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

(e) **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:

1. ONE. Little or no history of attacking this type of asset.

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

3. THREE. Recent, credible threats against this type of asset.

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

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

(f) **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.

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

2. 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.

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

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

5. FIVE. No perimeter protection, defense in depth, or detection capability; surveillance can be conducted “at will.”

(g) **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:

1. ONE. Cannot be recognized under any conditions — except by experts; little useful or no open source information, architecture, or signage exists.

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

3. 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.

4. 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.

(h) **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.

1. ONE. No people present or infrequently populated by very few people; contains people that the terrorist group considers desirable to avoid harming.

2. TWO. Sparsely populated; prone to having small groups or individuals, little target value based on demographics of occupants.

3. THREE. Moderate number of people, known target group may be present; no special segment necessary for mission accomplishment.

(i) **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).

1. ONE. Asset is adjacent to assets that are undesirable to attack or damage.

2. TWO. Asset is isolated, no access to other assets.

3. THREE. Asset is isolated; however, access to this asset would allow access to other assets.

(j) 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 one 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.

(3) **CARVER**

(a) CARVER is used in target analysis and technical appreciation to assess mission, validity, and requirements. CARVER identifies the most critical assets, choke points, and critical damage points. Bulk electric power supply, bulk petroleum supply, and mass telecommunications are three examples of this.

(b) The acronym CARVER represents the following:

1. 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:

a. How rapidly shall the impact of asset destruction affect the unit's essential functions?

b. What percentage of output and essential functions is curtailed by asset damage?

c. Is there an existence of substitutes for the output product or service?

d. What is the number of assets and their position in the system or complex flow diagram?

e. Criticality asks the question: How critical is the asset to your mission accomplishment?

2. 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?

3. 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?

4. 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:

a. The nature of the construction of the target.

b. The assets available (manpower, transportation, weapons, explosives, and equipment) to defend the asset.

c. Vulnerability asks the questions: Is the asset literally hardened or guarded? Are measures in place to mitigate any threat?

5. 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 themes be contradicted or reinforced? Will exfiltration and evasion be helped or hurt? Will the enemy population be alienated from its government, or will 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 terrorism or demoralization, and associated mission degradation?

6. Recognizability. The degree that a target can be recognized under varying weather, light, and seasonal conditions without confusion with other targets or components.

a. 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.

b. Recognizability asks the question: Can the enemy recognize the target for what it truly is and its importance?

(c) 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:

1. For strategic level analysis, list systems and subsystems.

2. 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.

(d) After completing the matrix for all assets, total the scores and then rank order those totals to prioritize vulnerabilities.

(e) The following are basic mitigation tips to address four of the six CARVER components:

1. 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.

2. Reduce accessibility. Reduce access, both physical and through cyberspace, 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.

3. 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.

4. 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.

d. Criticality Assessment Matrix

(1) 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.

(2) 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.”

(3) It is important to note that situational changes can affect the criticality of an asset (e.g., different phases of an operation). Also, the loss of assets with a certain capability may increase the criticality of those remaining in an operation.

(4) Another important item to note is that the DCIP provides for the assignment of Tier levels (1 through 3) but does not prioritize assets within these tiers. By definition, the loss or degradation of these assets has been determined by the mission owner (frequently at the combatant-command level) to cause mission failure or degradation at the strategic or operational level. Thus commanders must ensure appropriate levels of protection are provided to these assets regardless of any local criticality determination.

2. Threat Assessment

The TA system is vital for communicating terrorism threat 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. Threat analysis provides the intelligence officer with information upon which to base warnings. 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. A standardized format for the dynamic 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. Terrorist threat warnings for DOD use two mechanisms: IC warning products (alerts, advisories, assessments, and memorandums) and defense terrorism warning reports (DTWRs) and defense terrorism awareness message (DTAM). The interagency intelligence committee on counterterrorism (IICT) is authorized to provide national-level terrorism warnings to USG organizations and customers. An IICT alert warns of a credible, specific, imminent terrorist threat against US personnel, facilities, or interests. Information in an alert must be specific and credible enough to permit implementation of local security measures. It expires in 30 days without extension. An IICT advisory warns of a credible terrorist threat to US personnel, facilities, or interests, with information which is general in both timing and target, or details significant trends and developments in terrorism which may lead to an increased threat situation. It expires in 45 days but may have one extension. An IICT assessment serves multiple functions: may disseminate warnings of credible but non-specific threat information, or may provide in-depth analysis on a specific terrorism topic trend or development for decision-making and policy audience as appropriate. These assessments do not expire. An IICT memorandum is a short form assessment. The DOD defense indications and warning system is an independent system in which DOD members at any level may initiate unilateral threat warnings. These are the DTWR and the DTAM. Warnings within DOD system generally stay within the system and are primarily for use by DOD components. A DTWR addresses a terrorist group being operationally active and specifically targeting US interests, specific, credible information of attack timing and targets, maximum classification is SECRET/NOFORN, coordinated with the combatant commands when time allows, signed by the J-2 and is active for 30 days with one 30 day extension. A DTAM summarizes recent credible threat reporting concerning DOD or US interests, general in timing and/or target information, maximum classification is SECRET/NOFORN, coordinated with the combatant commands and signed by the J-2 with no expiration date. It can/should be updated.

a. Threat Assessment Requirements and Activities

(1) 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.

(2) **Annual Threat Assessment.** Commanders shall, at least annually, prepare or obtain 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 including WMD.

(a) **Threat Levels.** Threat levels are determined based on the presence of a combination of factors. **Terrorist threat levels do not address when a terrorist attack will occur and do not specify a FPCON status.** Issuance of a terrorist threat level judgment is not a warning notice. Formal terrorism warning notices are issued separately. There are four terrorist threat levels:

1. **LOW.** No group is detected or the group activity is non-threatening.
2. **MODERATE.** Terrorists are present but there are no indications of anti-US activity. The operating environment favors the host nation/US.
3. **SIGNIFICANT.** Anti-US terrorists are present and attack personnel as their preferred method of operation or a group uses large casualty producing attacks as their preferred method but has limited operational activity. The operating environment is neutral.
4. **HIGH.** Anti-US terrorists are operationally active and use large casualty producing attacks as their preferred method of operation. There is a substantial DOD presence and the operating environment favors the terrorist.

(3) **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.

(4) Both installation and unit commanders shall assess the terrorist threat for probability and severity of occurrence (capability and intent). 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 (capability and

intent) 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.

(5) TAs of specific operations, missions or events may also be conducted to identify specific threats to the conduct of those activities.

(6) 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.

3. Vulnerability Assessment

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 (AT) 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. If the capability and intent of the threat warrants attention to the vulnerability of an asset, then reducing the vulnerability of an asset reduces the potential risk to the asset. Developing and assessing terrorist threat capability/threat priority matrix (Figure E-1) is one method for commanders to assess probability and severity of occurrence of a terrorist attack; and to help set priorities in guarding against them.

a. Assessing Vulnerability

(1) 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 & Strategic Plan*, and DODI 2000.18, *DOD*

NOTIONAL ASSESSING TERRORIST THREAT CAPABILITY THREAT/PRIORITY MATRIX

Threat Capability	Weapon	Delivery Method	Threat Probability (Highest # is most probable)	Threat Severity (Highest # is most severe)	Threat Priority (Probability x Severity)	Threat Priority Inside Perimeter **	Threat Priority Outside Perimeter **
Vehicle Bomb	220 lbs *	(motorcycle, car, truck, boat, plane)	13	6	78	1	2
	1,000 lbs		12	7	84	NA	1
	20,000 lbs		4	12	48	NA	4
Mail Bomb	2 lbs	Package	10	2	20	8	NA
Sniper	7.62mm/308 Cal.	Sniper	11	1	11	9	10
Standoff	Mortar	Hasty Attack	9	5	45	4	NA
Weapons	RPG	Hasty Attack	8	4	32	6	8
Man Portable Air Defense Systems	Surface-to-air (SA)7, SA16	Attack against aircraft in arrival/ departure footprint	5	9	45	NA	6
Pier Side Ship Ship	Surface Bomb	Boat	7	10	70	2	3
	Sub-surface Bomb	Divers	6	8	48	3	4
WMD	Anthrax	Letter	1	3	3	10	NA
	Nerve Agent/ Toxic Industrial Chemical	Dispersed up wind of	2	13	26	7	9
	Chemical /Biological Poison	Food/Water	3	11	33	5	7

This example matrix is used to assess threat capabilities and determine which threats to guard against in priority. It describes threats at a notional installation that for illustration purposes has both a pier and airfield.

* Assumption that a 220 pound bomb is largest that could be concealed from security forces controlling access and transported inside the perimeter of an installation.

**Lowest number is highest priority threat inside and outside the perimeter.

Figure E-1. Notional Assessing Terrorist Threat Capability Threat/Priority Matrix

Installation Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive Emergency Response Guidelines.

(2) 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:

- (a) List assets and the threats against those assets.
- (b) Determine criteria to be used to assess assets against.
- (c) Train assessment team on assessment intent and methodology.
- (d) Assessment team conducts assessment.
- (e) Consolidate and review assessment results.

(3) The DOD VA Benchmarks are another excellent tool available for local (base) VAs. This is a comprehensive benchmark that is directly linked to DODI 2000.16, *DOD Antiterrorism Standards*, and produces a product similar to a JSIVA. Other resources can assist commanders in AT planning and risk management and can be accessed on ATEP on Army Knowledge Online/Defense Knowledge Online.

(4) Core Vulnerability Assessment Management Program

(a) CVAMP is an automated and Web-based means of managing a command's vulnerabilities and associated funding requirements. CVAMP key capabilities include:

1. 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.
2. Provide capability of receiving observations directly from the Vulnerability Assessment Reporting and Analysis Tool.
3. Document a commander's risk assessment decision for each vulnerability.
4. Track the status of known vulnerabilities until mitigated.
5. Provide a tool to assist in prioritizing vulnerabilities via a weighted scale based on user input.

6. Provide commanders a vehicle to identify requirements to the responsible chain of command.

7. Provide the ability to roll vulnerability data into a resource requirement.

8. 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.

a. Allow for prioritization of funding requests as well as provide a tool to assist in this process based on user input.

b. Provide a ready reference to track the status of installations and activities by FPCON and/or terrorism threat level.

(b) Registration for CVAMP is initiated from a link on CVAMP’s Login Page that is accessible via the SECRET Internet Protocol Router Network (SIPRNET). The registrant must have a valid SIPRNET email address in order to successfully register for CVAMP. During the registration process, system administrators in the registrant’s chain-of-command are notified of the registration request. The system administrators grant access to CVAMP and 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. System operation is hierarchical and process driven, and incorporates drop-down menus that assist data entry (e.g., create, review, modify) and program administration. Initial CVAMP-related roles and their permissions are:

1. 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.

2. ATO. Capability to create vulnerability assessments, vulnerability, and funding requests.

3. Resource Manager. Capability to read and/or write to all funding requests.

4. Assessor. Capability to create observations associated with a vulnerability assessment.

5. System Administrator. Capability to assign and manage roles within immediate organization and one level down.

6. Users should contact their local/and or next higher headquarters CVAMP administrators to establish their roles within CVAMP.

4. Risk Assessment

The 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.

a. Risk Assessment Methodology

(1) 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.

(a) **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.).

(b) **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.

(c) **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, CBRN vulnerability); the findings of these functional area vulnerability assessments must be included in the overall installation assessment.

(2) 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.

(3) 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.

(4) 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.

b. Assessing Risk—A Practical Exercise

(1) 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.

(2) 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 E-2.

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 × V × TP)
Small arms fire	9	1	9	81
Car or truck bomb	9	8	6	432
CBRN weapon	9	8	1	72

Figure E-2. Example Asset Risk Assessment Table

(a) **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, CBRN weapons, etc. Use the information from Chapter V, “Antiterrorism Programs.”

(b) **Criticality.** Obtained from the information gathered in Chapter V, “Antiterrorism Programs.”

(c) **Vulnerability.** Obtained from the information gathered in Chapter VI, “Terrorist Incident Response.”

(3) **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 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 CBRN attack means are both high vulnerabilities because the ventilation system is unfiltered.

(4) 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.

c. Risk Assessment

(1) Figure E-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.

(2) The risk can also be represented graphically using the RA graph, Figure E-3. 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).

(3) 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:

- (a) What is the installation's mission? How important is that mission to overall US military objectives in the region? (Criticality Assessment)
- (b) What resources are available for AT activities on the installation? (VA)
- (c) 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)

d. Completing the Process—Risk Management

(1) The end products of the above process shall be the identification of areas and assets that present the most risk 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.

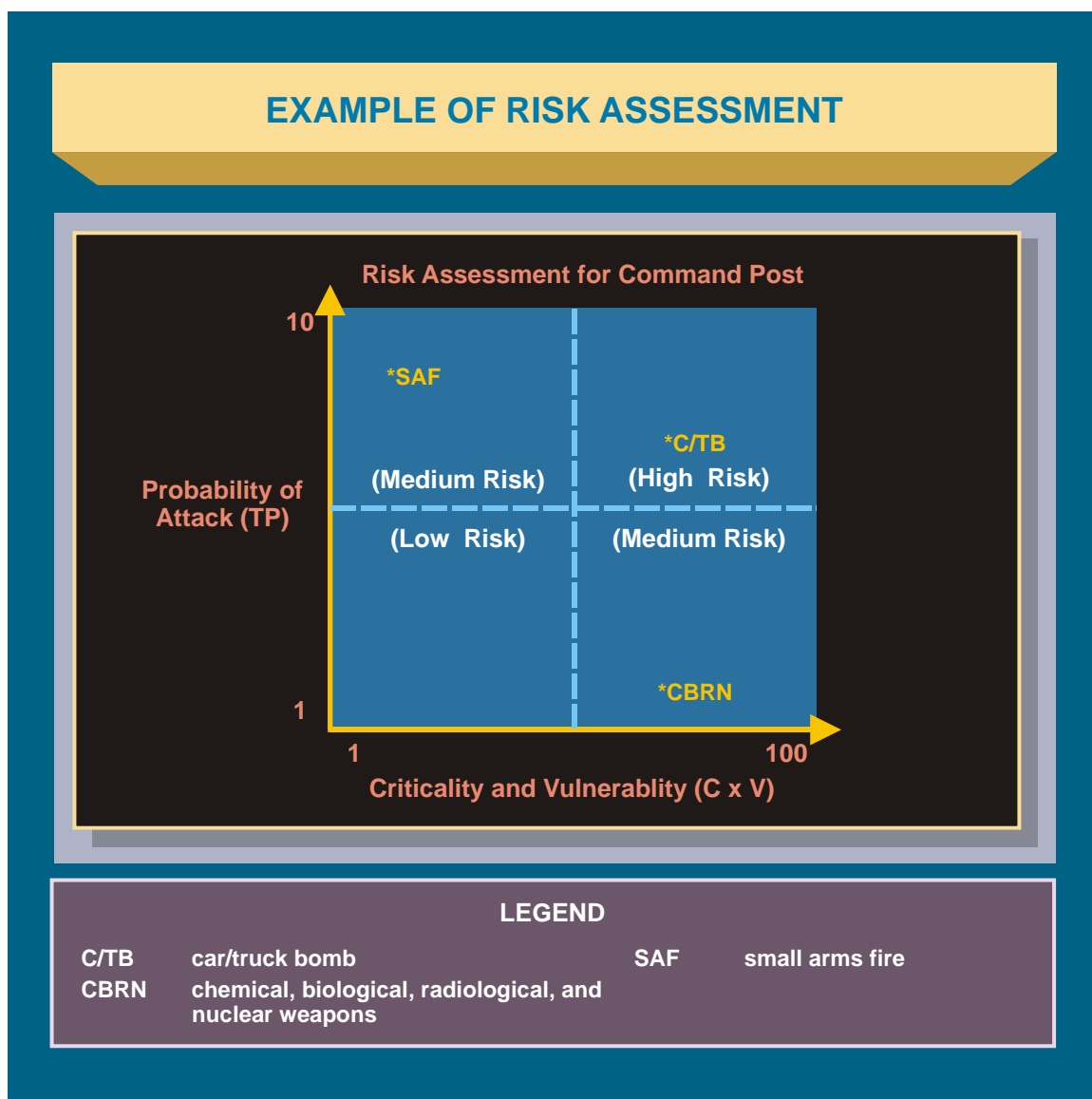


Figure E-3. Example of Risk Assessment

(2) 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.

(3) 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?

(a) 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.

(b) 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.

(4) 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).

(5) CVAMP shall be employed to recover vulnerability and risk assessment data and related resource requirements or requests.

e. 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 commands, and Service intelligence elements 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 are established by DIA, but the GCC may set terrorism threat levels for specific personnel, family members, units, installations, or geographic regions in countries within the AOR, using the definition and criteria established by DIA.

APPENDIX F REFERENCES

The development of JP 3-07.2 is based upon the following primary references:

1. General

- a. *Unified Command Plan*.
- b. Presidential Military Order of November 13, 2001, *Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism*.
- c. Public Law 107–314—Dec. 2, 2002, *Bob Stump National Defense Authorization Act for Fiscal Year 2003*.
- d. Public Law 107–296—Nov. 25, 2002, *Homeland Security Act of 2002*.
- e. United States Department of State, *Patterns of Global Terrorism* 2008.
- f. *National Strategy for Combating Terrorism*, February 2006.
- g. *National Security Strategy of the United States of America*.
- h. *National Strategy for Homeland Security*, October 2007.
- i. *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*, February 2003.
- j. *National Military Strategic Plan for the War on Terrorism*, February 2006.
- k. *US National Strategy for Public Diplomacy and Strategic Communication*, December 2006.
- l. *Combating Maritime Terrorism Strategic and Performance Plan*, June 2008.
- m. *United States Government Interagency Domestic Terrorism Concept of Operations Plan*, January 2001.
- n. *Operational Law Handbook (2007)*.
- o. Memorandum of Understanding Between the Department of State, Bureau of Diplomatic Security, and Department of Defense/CI Field Activity Concerning Force Protection Detachments, May 9, 2003.
- p. Laura Clark and William E. Algaier, *Surveillance Detection: The Art of Prevention*, (St. Louis: Cradle Press, 2007).

q. Col Shannon D. Jurens, USAF, “Slashing the Enemy’s Achilles Heel: Using Surveillance Detection to Prevent Terrorist Attacks,” *The Guardian*, Winter 2010, Volume 12, Issue 3.

r. Donald J. Hanle, *Terrorism: The Newest Face of Warfare* (Washington: Pergamon-Brassey’s International Defense Publishers, Inc., 1989).

2. DOD Publications

a. DODD 2000.12, *DOD Antiterrorism (AT) Program*.

b. DOD O-2000.12-H, *DOD Antiterrorism Handbook*.

c. DODD 3020.40, *Defense Critical Infrastructure Program (DCIP)*.

d. DODD 3025.15, *Military Assistance to Civil Authorities*.

e. DODD 4500.54E, *DOD Foreign Clearance Program (FCP)*.

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

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

h. DODD 5240.1, *DOD Intelligence Activities*.

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

j. DODI S-5240.15, *The Force Protection Response Group (FPRG)*.

k. DODI 2000.16, *DOD Antiterrorism Standards*.

l. DODI 2000.18, *Department of Defense Installation Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive Emergency Response Guidelines*.

m. DODI O-2000.22, *Designation and Physical Protection of DOD High Risk Personnel (HRP)*.

n. DODI 3020.41, *Contractor Personnel Authorized to Accompany the US Armed Forces*.

o. DODI 5240.6, *Counterintelligence (CI) Awareness, Briefing, and Reporting Programs*.

p. DODI 5240.22, *Counterintelligence Support to Force Protection*.

q. DODI 5525.07, *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*.

r. DODI 6055.17, *DOD Installation Emergency Management (IEM) Program*.

3. CJSC Publications

a. CJCSI 3121.01B, *Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces*.

b. CJCSI 5120.02B, *Joint Doctrine Development System*.

c. CJCSI 5261.01F, *Combating Terrorism Readiness Initiatives Fund*.

d. CJCSI 7401.01E, *Combatant Commander Initiative Fund*

e. CJCS Guide 5260, *Self-Help Guide to Antiterrorism*.

f. Chairman of the Joint Chiefs of Staff Manual 3122.03B *Joint Operation Planning and Execution System Volume II, Planning Formats*.

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

h. JP 1-0, *Personnel Support to Joint Operations*.

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

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

k. JP 2-03, *Geospatial Intelligence Support to Joint Operations*.

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

m. JP 3-05, *Joint Special Operations*.

n. JP 3-08, *Interorganizational Coordination During Joint Operations*.

o. JP 3-10, *Joint Security Operations in Theater*.

p. JP 3-11, *Operations in Chemical, Biological, Radiological, and Nuclear (CBRN) Environments*.

q. JP 3-13, *Information Operations*.

r. JP 3-13.1, *Electronic Warfare*.

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

- t. JP 3-24, *Counterinsurgency Operations*.
- u. JP 3-26, *Counterterrorism*.
- v. JP 3-27, *Homeland Defense*.
- w. JP 3-38, *Civil Support*.
- x. JP 3-40, *Combating Weapons of Mass Destruction*.
- y. JP 3-41, *Chemical, Biological, Radiological, and Nuclear Consequence Management*.
- z. JP 4-10, *Operational Contract Support*.

APPENDIX G

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, *Antiterrorism*, 14 April 2006.

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//JDJ10//

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 Publications

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 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, Defense Foreign Liaison/IE-3, 200 MacDill Blvd., Bolling AFB, Washington, DC 20340-5100.

c. CD-ROM. Upon request of a JDDC member, the Joint Staff J-7 will produce and deliver one CD-ROM with current joint publications.

GLOSSARY

PART I-ABBREVIATIONS AND ACRONYMS

AFOSI	Air Force Office of Special Investigations
AOR	area of responsibility
ASD(HD&ASA)	Assistant Secretary of Defense (Homeland Defense and Americas' Security Affairs)
AT	antiterrorism
ATCC	Antiterrorism Coordinating Committee
ATEP	Antiterrorism Enterprise Portal
ATO	antiterrorism officer
C2	command and control
CA	criticality assessment
CARVER	criticality, accessibility, recuperability, vulnerability, effect, and recognizability
CBRN	chemical, biological, radiological, and nuclear
CbT	combating terrorism
CCDR	combatant commander
CCIF	Combatant Commander Initiative Fund
CI	counterintelligence
CIA	Central Intelligence Agency
CIP	critical infrastructure protection
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSM	Chairman of the Joint Chiefs of Staff manual
COM	chief of mission
COOP	continuity of operations
CT	counterterrorism
CTDB	combating terrorism database
CTKB	combating terrorism knowledge base
CVAMP	Core Vulnerability Assessment Management Program
DBT	design basis threat
DCIP	Defense Critical Infrastructure Program
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DOJ	Department of Justice
DOMEX	document and media exploitation
DOS	Department of State
DTA	dynamic threat assessment
DTAM	defense terrorism awareness message

DTRA	Defense Threat Reduction Agency
DTWR	defense terrorism warning report
DVD	digital video disc
ECP	entry control point
EFP	explosively formed projectile
EO	executive order
EOC	emergency operations center
EOD	explosive ordnance disposal
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FP	force protection
FPCON	force protection condition
FPD	force protection detachment
GCC	geographic combatant commander
GEOINT	geospatial intelligence
HAZMAT	hazardous materials
HD	homeland defense
HN	host nation
HNS	host-nation support
HQ	headquarters
HRB	high-risk billet
HRP	high-risk personnel
HS	homeland security
HUMINT	human intelligence
IC	intelligence community
IICT	Interagency Intelligence Committee on Counterterrorism
ICS	incident command system
IED	improvised explosive device
IO	information operations
IPB	intelligence preparation of the battlespace
IR	information requirement
IRA	Provisional Irish Republican Army
ISR	intelligence, surveillance, and reconnaissance
J-2	intelligence directorate of a joint staff
JFC	joint force commander
JITF-CT	Joint Intelligence Task Force for Combating Terrorism
JOPEs	Joint Operation Planning and Execution System
JP	joint publication
JSA	joint security area
JSC	joint security coordinator

JSIVA	Joint Staff Integrated Vulnerability Assessment
JTF	joint task force
JTTF	joint terrorism task force
LE	law enforcement
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
NCTC	National Counterterrorism Center
NGO	nongovernmental organization
NIMS	National Incident Management System
NJTTF	National Joint Terrorism Task Force
NRF	National Response Framework
OASD(PA)	Office of the Assistant Secretary of Defense (Public Affairs)
OC	operations center
OIF	Operation IRAQI FREEDOM
OP	observation post
OPLAN	operation plan
OPSEC	operations security
PA	public affairs
PAO	public affairs officer
PIR	priority intelligence requirement
PPBE	Planning, Programming, Budgeting, and Execution
R&R	rest and recuperation
RA	risk assessment
RAM	random antiterrorism measure
RM	risk management
ROE	rules of engagement
RUF	rules for the use of force
SAR	suspicious activity report
SecDef	Secretary of Defense
SECSTATE	Secretary of State
SIGINT	signals intelligence
SIPRNET	SECRET Internet Protocol Router Network
SIR	specific information requirement

SJA	staff judge advocate
SOFA	status-of-forces agreement
SOP	standing operating procedure
TA	threat assessment
TACON	tactical control
TTP	tactics, techniques, and procedures
UAV	unmanned aerial vehicle
UFC	Unified Facilities Criteria
USACIDC	United States Army Criminal Investigation Command
USC	United States Code
USCG	United States Coast Guard
USG	United States Government
VA	vulnerability assessment
VBIED	vehicle-borne improvised explosive device
WMD	weapons of mass destruction

PART II—TERMS AND DEFINITIONS

Unless otherwise annotated, this publication is the proponent for all terms and definitions found in the glossary. Upon approval, JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, will reflect this publication as the source document for these terms and definitions.

advance guard. Detachment sent ahead of the main force to ensure its uninterrupted advance; to protect the main body against surprise; to facilitate the advance by removing obstacles and repairing roads and bridges; and to cover the deployment of the main body if it is committed to action. (Approved for incorporation into JP 1-02 with JP 3-07.2 as the source JP.)

antiterrorism. Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include rapid containment by local military and civilian forces. Also called **AT**. (Approved for incorporation into JP 1-02.)

biometrics. The process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics. (JP 1-02. SOURCE: JP 2-0)

chemical, biological, radiological, nuclear, and high-yield explosive hazards. None. (Approved for removal from JP 1-02.)

combating terrorism. Actions, including antiterrorism and counterterrorism, taken to oppose terrorism throughout the entire threat spectrum. Also called **CbT**. (JP 1-02. SOURCE: JP 3-26)

countersurveillance. All measures, active or passive, taken to counteract hostile surveillance. (Approved for incorporation into JP 1-02 with JP 3-07.2 as the source JP.)

counterterrorism. Actions taken directly against terrorist networks and indirectly to influence and render global and regional environments inhospitable to terrorist networks. Also called **CT**. (JP 1-02. SOURCE: JP 3-26)

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. SOURCE: JP 3-07.2)

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. (JP 1-02. SOURCE: JP 3-07.2)

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**. (JP 1-02. SOURCE: JP 3-07.2)

dynamic threat assessment. An intelligence assessment developed by the Defense Intelligence Agency that details the threat, capabilities, and intentions of adversaries in each of the priority plans in the Contingency Planning Guidance. Also called **DTA**. (JP 1-02. SOURCE: JP 2-0)

force protection. Preventive measures taken to 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**. (JP 1-02. SOURCE: JP 3-0)

force protection condition. A Chairman of the Joint Chiefs of Staff-approved standard for identification of and recommended responses to terrorist threats against US personnel and facilities. Also called **FPCON**. (Approved for incorporation into 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**. (JP 1-02. SOURCE: JP 3-07.2)

hostage. None. (Approved for removal from 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. SOURCE: JP 3-15.1)

initial response force. The first unit, usually military police, on the scene of a terrorist incident. (JP 1-02. SOURCE: JP 3-07.2)

installation. None. (Approved for removal from JP 1-02.)

installation commander. None. (Approved for removal from JP 1-02.)

insurgency. The organized use of subversion and violence by a group or movement that seeks to overthrow or force change of a governing authority. Insurgency can also refer to the group itself. (JP 1-02. SOURCE: JP 3-24)

intruder. None. (Approved for removal from JP 1-02.)

military intervention. None. (Approved for removal from 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**. (JP 1-02. SOURCE: JP 3-07.2)

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 adversary 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. SOURCE: JP 3-13.3)

prevention. In space usage, measures to preclude an adversary's hostile use of United States or third-party space systems and services. Prevention can include diplomatic, economic, and political measures. (Approved for incorporation into JP 1-02 with JP 3-14 as the source JP.)

proactive measures. None. (Approved for removal from JP 1-02.)

proclamation. None. (Approved for removal from JP 1-02.)

protection. 1. Preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area. (JP 3-0) 2. In space usage, active and passive defensive measures to ensure that United States and friendly space systems perform as designed by seeking to overcome an adversary's attempts to negate them and to minimize damage if negation is attempted. (JP 1-02. SOURCE: JP 3-14)

risk assessment. The identification and assessment of hazards (first two steps of risk management process). Also called **RA**. (Approved for incorporation into JP 1-02 with JP 3-07.2 as the source JP.)

risk management. The process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk cost with mission benefits. Also called **RM**. (JP 1-02. SOURCE: JP 2-0)

safe house. An innocent-appearing house or premises established by an organization for the purpose of conducting clandestine or covert activity in relative security. (Approved for incorporation into JP 1-02 with JP 3-07.2 as the source JP.)

security alert team. None. (Approved for removal from JP 1-02.)

special weapons. None. (Approved for removal from JP 1-02.)

tactical security. None. (Approved for removal from JP 1-02.)

terrorism. The unlawful use of violence or threat of violence to instill fear and coerce governments or societies. Terrorism is often motivated by religious, political, or other ideological beliefs and committed in the pursuit of goals that are usually political. (Approved for incorporation into JP 1-02.)

terrorist. None. (Approved for removal from JP 1-02.)

terrorist group. None. (Approved for removal from 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 four threat levels: **LOW**, **MODERATE**, **SIGNIFICANT**, and **HIGH**. 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.) (Approved for incorporation into 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. SOURCE: JP 3-07.2)

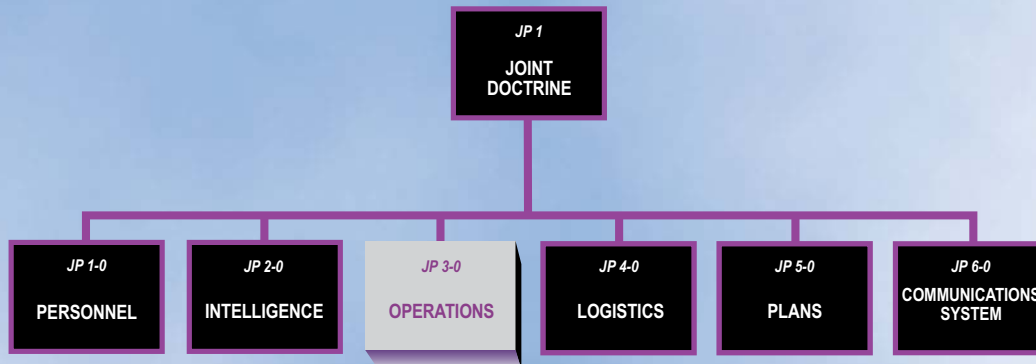
threat assessment. In antiterrorism, examining the capabilities, intentions, and activities, past and present, of terrorist organizations as well as the security environment within which friendly forces operate to determine the level of threat. Also called **TA**. (Approved for inclusion in JP 1-02.)

threat and vulnerability assessment. In antiterrorism, the pairing of a facility's threat analysis and vulnerability analysis. (JP 1-02. SOURCE: JP 3-07.2)

vehicle-borne improvised explosive device. A device placed or fabricated in an improvised manner on a vehicle incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. Otherwise known as a car bomb. Also called **VBIED**. (JP 1-02. SOURCE JP 3-10)

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**. (JP 1-02. SOURCE: JP 3-07.2)

JOINT DOCTRINE PUBLICATIONS HIERARCHY



All joint publications are 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:

