COMBINED ARMS RESEARCH LIBRARY
FORT LEAVENWORTH, KS
3 1695 00676 9053

cy2

Joint Pub 3-07.2

Joint Tactics, Techniques, and Procedures for Antiterrorism

17 March 1998



This second edition of Joint Pub 3-07.2, "Joint Tactics, Techniques, and Procedures for Antiterrorism," represents a significant improvement in the key area of force protection.

Joint Pub 3-07.2 provides tactics, techniques, and procedures for the conduct of US antiterrorism operations in joint operations. It discusses US national policy, explains key responsibilities for antiterrorism actions, and covers key command and control relationships. The guidance contained herein provides joint force commanders with the knowledge needed to organize, plan, train for, and conduct antiterrorism operations.

Experience has shown that force protection must be a high priority for any commander. Antiterrorism is essential to a force protection program. Commanders must understand the content of this publication and bring it to bear during joint and multinational operations. Please ensure the widest distribution of this and other joint publications, and promote their use at every opportunity.

HENRY H. SHELTON
Chairman
of the Joint Chiefs of Staff

PREFACE

1. Scope

This publication sets forth the tactics, techniques, and procedures governing the joint conduct of US antiterrorism operations. It provides a basis for understanding US national policy and general objectives relating to antiterrorism and explains important Department of Defense and US Government agency command and control relationships. In addition, it outlines basic US military antiterrorism capabilities and provides commanders with guidance on how to organize, plan, and train for the employment of US forces in interagency and multinational antiterrorism operations.

2. Purpose

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

3. Application

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

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

Intentionally Blank

TABLE OF CONTENTS

PAGE

EXECUTIVE SUMMARY vii

CHAPTER I
INTRODUCTION

- General I-1
- Purpose I-1
- Force Protection and Antiterrorism Relationship I-2
- Overview of DOD Responsibility I-2
- DOD Role I-3

CHAPTER II
TERRORIST THREAT

- Overview II-1
- Terrorist Tactics II-1
- Terrorist Groups II-5
- Terrorist Organization II-6
- Terrorist Targets — Americans II-9
- Domestic Terrorism II-10
- Terrorism Against the US Military II-10

CHAPTER III
LEGAL CONSIDERATIONS

- General III-1
- US Policy III-1
- Lead Agencies III-2

SECTION A. LEGAL CONSIDERATIONS: AUTHORITY III-3
- Criminal Actions III-3
- Jurisdiction III-4
- Commander's Authority III-4

SECTION B. LEGAL CONSIDERATIONS: PERMISSIBLE LIMITS OF MILITARY SUPPORT TO CIVIL AUTHORITIES III-4
- General III-4
- Statutory Authorizations Allowing the Use of the Military III-4

SECTION C. LEGAL CONSIDERATIONS: JURISDICTION AND AUTHORITY FOR HANDLING TERRORIST INCIDENTS III-6
- Jurisdictional Status of Federal Property in the United States, Its Territories, and Its Possessions III-6
- Federal Authority in the United States, Its Territories, and Its Possessions III-8
- Federal and State Concurrent Authority III-8
- Jurisdictional Authority III-8

SECTION D. LEGAL CONSIDERATIONS: FEDERAL AGENCIES AND THE MILITARY III-8
- Overview III-8
- The National Security Council III-8
- The Committee to Combat Acts of Terrorism III-9
- Department of Justice III-9
- Federal Bureau of Investigation III-9
- Department of Defense III-9
- Military Authority III-9
- Military Installation Commander's Responsibilities III-11

CHAPTER IV
ANTITERRORISM PROGRAM; INSTALLATION, BASE, SHIP, UNIT, AND PORT

- Overview of Program Concept IV-1
- Implementing the Concept IV-7
- Threat Conditions IV-9
- Combatant Commander's Responsibility IV-9

CHAPTER V
INTELLIGENCE, COUNTERINTELLIGENCE, AND THREAT ANALYSIS

SECTION A. INTELLIGENCE AND COUNTERINTELLIGENCE V-1
- Intelligence and Counterintelligence Support V-1
- Sources V-1
- Responsibilities of US Government Lead Agencies V-2
- Information Requirements V-5

SECTION B. THREAT ASSESSMENT V-5
- Preparation of Threat Analysis V-5
- Preparation of Criticality and Vulnerability Assessments V-8
- Drills and Exercises V-9

CHAPTER VI
CRISIS MANAGEMENT EXECUTION

- General VI-1
- Initial Response VI-1
- Response VI-2
- Special Considerations VI-5

CHAPTER VII
PREVENTIVE MEASURES AND CONSIDERATIONS

- Commander's Responsibility VII-1
- AT Force Protection in High-Risk Areas VII-1
- Tactical Force Protection VII-9

APPENDIX

A Vulnerability Assessment A-1
B Personal Protective Measures Against Terrorism B-1
C Very Important Person and Senior Officer Security Measures C-1
D Building Security Procedures D-1
E Lock Security E-1
F Telephone Call Procedures F-1
G Crisis Management Plan Format G-1
H Crisis Management Plan Checklist H-1
J THREATCON System J-1
K Explosive Device Procedures K-1
L Jurisdictional Authority for Handling Terrorist Incidents L-1
M Public Affairs Checklist M-1
N Military Working Dogs N-1
O References O-1
P Administrative Instructions P-1

GLOSSARY

Part I Abbreviations and Acronyms GL-1
Part II Terms and Definitions GL-3

FIGURE

I-1 Antiterrorism & Counterterrorism I-1
II-1 Examples of Terrorist Objectives II-1
II-2 Common Terrorist Tactics II-2
II-3 Categories of Terrorist Groups II-6
II-4 Structure Pyramid of a Typical Terrorist Organization II-7
III-1 Lead Agencies for Terrorist Incidents III-2
III-2 Federal Territorial Jurisdiction Categories III-7
III-3 Approval for Use of Military Force III-10
IV-1 Antiterrorism Program Concept IV-2
IV-2 Operations Security Antiterrorism Objectives IV-4
IV-3 Antiterrorism Program Functions for Installation Commanders IV-8
IV-4 Crisis Management Participants IV-9
IV-5 On-Site Operational Response Structure IV-10
V-1 Sources of Intelligence and Counterintelligence V-1
V-2 Information Requirements V-6
V-3 Threat Level V-8

Table of Contents

VI-1 Crisis Management Execution Considerations VI-2
VI-2 Terrorist Incident Phases VI-3
VI-3 Response to a Terrorist Incident VI-4
VI-4 Special Considerations VI-5
VII-1 Fortification Materials VII-3
VII-2 Security Force Equipment VII-4
VII-3 Principles of Riot Control VII-9
L-1 Jurisdictional Authority for Handling Terrorist Incidents L-2

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Discusses US National Policy and General Objectives**
- **Explains Important Department of Defense and US Government Agency Command and Control Relationships**
- **Outlines Basic US Military Antiterrorism Capabilities**
- **Provides Guidance for the Employment of US Forces in Antiterrorism Operations**
- **Explains Legal Considerations Affecting the Implementation of Successful Programs**
- **Describes Sources of Intelligence and Counterintelligence**

Combatting Terrorism

Combatting terrorism involves actions taken to oppose terrorism throughout the entire threat spectrum.

Specific tactics, techniques, and procedures govern the joint conduct of US antiterrorism operations. **Combatting terrorism is an element of force protection** — a security program designed to protect Service members, civilian employees, family members, facilities, and equipment in all locations and situations. Combatting terrorism involves actions (including antiterrorism and counterterrorism) taken to oppose terrorism throughout the entire threat spectrum. Antiterrorism involves **defensive measures** used to reduce the vulnerability to terrorist acts, as opposed to counterterrorism which consists of offensive measures taken to prevent, deter, and respond to terrorism.

Department of Defense Roles and Responsibilities

The Department of Defense is responsible for protecting its own personnel, bases, deployed forces, equipment, and installations.

Every commander, regardless of echelon of command or branch of Service, **has an inherent responsibility for planning, resourcing, training, exercising, and executing antiterrorism measures** to provide for the security of the command. Likewise, every **military Service member**, **Department of Defense (DOD) employee**, **DOD independent contractor**, and **local national** hired by the Department of Defense, regardless of rank, has an inherent responsibility to **maintain vigilance for possible terrorist**

actions and to ensure that, where applicable, family members understand and employ antiterrorism tactics, techniques, and procedures. Specific DOD offices and agencies have been assigned specific responsibilities pertaining to combatting terrorism.

The Department of Defense assists lead agencies in combatting terrorism.

The Department of Defense is not the lead agency for combatting terrorism. **The Department of Defense is responsible for protecting its own personnel, bases, ships, deployed forces, equipment, and installations. The Department of Defense is also responsible for providing technical assistance or forces** when requested by the National Command Authorities. The lead agency is the **Department of State** for incidents outside the United States, the **Department of Justice** for incidents within the United States, and the **Department of Transportation and/or Federal Aviation Administration** for certain aviation incidents. The US Coast Guard is responsible for reducing the risk of maritime terrorist incidents and for manning the National Terrorism Hotline (1-800-424-8802) for reports of actual and/or potential domestic terrorism. All other Federal agencies possessing resources for responding to terrorism are linked together through agency command centers and crisis management groups to ensure effective coordination of the US response.

Terrorist Objectives and Tactics

Understanding the terrorist threat enables the commander to properly create and employ antiterrorism programs.

Terrorists frequently claim affiliation with **causes or political organizations** to give their actions a claim to respectability. **News media coverage is important to terrorists** who are attempting to incite public fear or gain attention for their cause. A determinant of **tactics and target selection** is the role the terrorist group perceives itself as playing. Terrorism can also be used as either an **overt or a covert aspect of a political movement** engaged in a power struggle within an existing political system. A terrorist group's selection of targets and tactics is also a function of the group's affiliation, level of training, organization, and sophistication.

Terrorists have a variety of objectives and tactics.

Examples of **objectives** of a terrorist attack are: to attract publicity for its cause, demonstrate the group's power, show the existing government's lack of power, extract revenge, obtain logistic support, or cause a government to overreact. Just as a terrorist incident may have several objectives, the tactics used may also be combined. The more **common**

tactics employed by terrorist groups are assassination, arson, bombing, hostage taking, kidnapping, hijacking, seizure, raids, sabotage, hoaxes, use of special weapons, and environmental destruction. Information systems and information infrastructures may also become targets of terrorist sabotage.

Legal Considerations

There are policy and jurisdictional responsibilities that apply to the Armed Forces.

A **command judge advocate** participates at all levels of foreign and domestic antiterrorism program planning and implementation. **The commander** of a combatant command, subunified command, joint task force, or component command must coordinate with the command judge advocate to determine the commander's authority in combatting terrorism and to provide a **basic understanding of the legal considerations** affecting the implementation of an effective antiterrorism program. In addition, statutory and regulatory restrictions may limit the type of assistance installation commanders may provide to civilian law enforcement officials investigating terrorist incidents and other crimes. Commanders should coordinate all proposed assistance with the Staff Judge Advocate to ensure compliance with such restrictions.

The Antiterrorism Program

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

The **antiterrorism program concept** represents an **integrated, comprehensive approach** within combatant commands and the Services to counter the terrorist threat to military installations, bases, facilities, equipment, and personnel. **The concept has two phases; proactive and reactive.** The proactive phase encompasses the planning, resourcing, preventive measures, preparation, awareness education, and training that take place before a terrorist incident. The reactive phase includes the crisis management actions taken to resolve a terrorist incident.

Counterterrorism

Counterterrorism (CT) is a highly specialized, resource-intensive mission. Certain special operations forces units maintain a high state of readiness to conduct CT operations and possess a full range of CT capabilities. Combatant commanders maintain designated CT contingency forces to respond to CT situations when national assets are not immediately available.

Intelligence and Counterintelligence

Intelligence and counterintelligence are the first line of defense in an antiterrorism program.

An effective **intelligence and counterintelligence program** is essential in order to identify the terrorist threat. Additionally, counterintelligence provides **warning of potential terrorist attacks** and provides **information for counterterrorism operations**. Effective intelligence and counterintelligence support requires effort, planning and direction, collection and analysis, production, investigations, and dissemination. The entire process is necessary to **provide decision makers with information and timely warning** upon which to take antiterrorism actions. The primary sources of intelligence and counterintelligence for the antiterrorism program are **open-source information, criminal records, government intelligence,** and **local information**.

Prevention

Preventive and protective security measures should be taken by military units and individual Service members.

The installation, base, ship, unit, or port **antiterrorism plan provides the mechanism to ensure readiness against terrorist attacks**. 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.

CONCLUSION

This publication sets forth the tactics, techniques, and procedures governing the joint conduct of US antiterrorism operations. It provides a basis for understanding US national policy and general objectives relating to antiterrorism and explains important DOD and US Government agency command and control relationships. In addition, it outlines basic US military antiterrorism capabilities and provides commanders with guidance on how to organize, plan, and train for the employment of US forces in interagency and multinational antiterrorism operations.

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

The term "terrorism" is defined as "the calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological." This definition is the foundation throughout this publication for the guidance to combatant commanders, subunified commanders, joint task force (JTF) commanders, and component commanders. Specific policy, directive guidance, standards, and procedures for the Department of Defense (DOD) combatting terrorism program is contained in DOD Directive (DODD) 2000.12, "DoD Combating Terrorism Program," DOD Instruction (DODI) 2000.14, "DoD Combating Terrorism Program Procedures," DODD O-2000.12-H, "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence," and DODI O-2000.16, "DoD Combating Terrorism Program Standards."

2. Purpose

Combatting terrorism involves actions including antiterrorism (AT) (defensive measures used to reduce the vulnerability to terrorist acts) and counterterrorism (CT) (offensive measures taken to prevent, deter, and respond to terrorism) taken to oppose terrorism throughout the entire threat spectrum. **This publication addresses only AT.** The following definitions, also shown in Figure I-1, are provided to assist in understanding the difference between AT and CT:

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

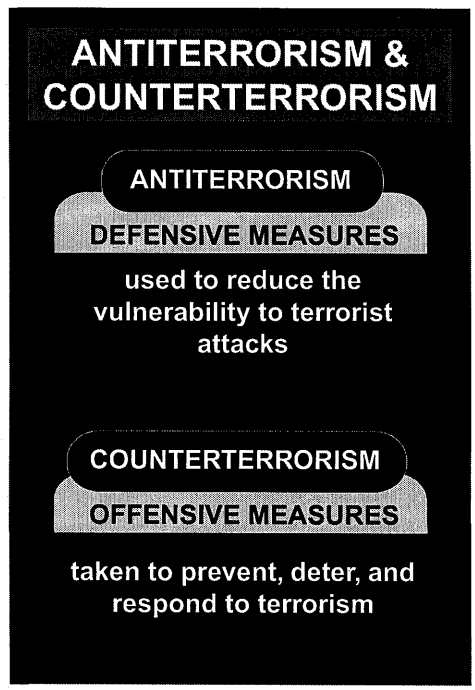


Figure I-1. Antiterrorism & Counterterrorism

b. **Counterterrorism** is offensive measures taken to prevent, deter, and respond to terrorism. Sensitive and compartmented CT programs are addressed in relevant National Security Decision Directives, National Security Directives, contingency plans, and other relevant classified documents.

3. Force Protection and Antiterrorism Relationship

As discussed throughout this publication, AT is a sub-element of combatting terrorism which is one of the four pillars of a broader concept called force protection (FP). **FP is** a security program designed to protect Service members, civilian employees, family members, facilities, and equipment in all locations and situations, **accomplished through planned and integrated application of combatting terrorism, physical security, operations security (OPSEC), and personal protective services** and supported by intelligence, counterintelligence, law enforcement, and other security programs.

4. Overview of DOD Responsibility

Every commander, regardless of echelon of command or branch of Service, has an inherent responsibility for planning, resourcing, training, exercising, and executing AT measures to provide for the security of the command. The importance of this responsibility is obvious in view of the varying levels and types of terrorist threats faced by US forces worldwide. Likewise, every military Service member, DOD employee, DOD independent contractor, and local national hired by the Department of Defense, regardless of rank, has an inherent responsibility to maintain vigilance for possible terrorist actions and to ensure that, where applicable, family members understand and employ AT tactics, techniques, and procedures. The Department of State (DOS) has also created a $2 million reward program to encourage this vigilance and the reporting of possible terrorist actions. Information on this program can be obtained through each Service's respective law enforcement agency.



Every commander has a responsibility for the security of the command against varying levels and types of terrorist threat.

5. DOD Role

The Department of Defense is not the lead agency for combatting terrorism; however, the Department of Defense is responsible for protecting its own personnel, bases, ships, deployed forces, equipment, and installations. At times, the Department of Defense is responsible for providing technical assistance or forces when requested by the National Command Authorities. Normally, the DOS is the lead agency for incidents outside the United States. However, on the Arabian Peninsula, the Department of Defense has been established as the lead agent in a memorandum of understanding (MOU) between the DOS and Department of Defense on the security of the Arabian Peninsula. The Department of Justice (DOJ) is the lead agency for incidents within the United States, and the Department of Transportation (DOT) and/or Federal Aviation Administration (FAA) serve as lead agency for certain aviation incidents. The following DOD offices and agencies have been assigned specific responsibilities pertaining to combatting terrorism:

a. **The Under Secretary of Defense for Acquisition and Technology** (USDA&T) shall:

- Provide a member to the DOD AT Coordinating Committee (ATCC) (and subcommittees as required), and a representative to the DOD Worldwide AT Conference.
- Ensure that the Defense Federal Acquisition Regulation (current edition) reflects current DOD AT and FP policy and addresses AT and FP security requirements for Defense contractors.
- Be the DOD official responsible for AT and FP technology development and expedite the application of new technology to meet AT and FP needs.

b. **The Under Secretary of Defense (Comptroller)** shall:

- Provide a member to the DOD ATCC (and subcommittees as required).
- Provide information and guidance to DOD components on displaying AT and FP resources within Planning, Programming, and Budgeting System (PPBS) program and budget submissions.
- Provide reports on AT and FP funds as requested by the Secretary of Defense and the Chairman of the Joint Chiefs of Staff (CJCS).

c. **The Under Secretary of Defense for Policy** shall:

- Provide appropriate members to the DOD ATCC (and subcommittees as required), the DOD Worldwide AT Conference, and an observer to the Overseas Security Policy Group (OSPG).
- Ensure that the Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict) (ASD[SO/LIC]) is supported in issuing the travel security advisory (TSA) message.

d. **The Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD[C3I])** shall:

- Provide policy and guidance for physical security programs, security and investigative matters, counterintelligence, DOD foreign counterintelligence, and information operations programs and work in conjunction with the ASD(SO/LIC) on matters pertaining to other elements of combatting terrorism programs.

- Review the DOD intelligence, counterintelligence, security, and information operations support provided in DODD 2000.12, "DoD Combating Terrorism Program," for compliance with DODD 5240.1, "DoD Intelligence Activities," and DODD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons."

- Monitor Defense Intelligence Agency (DIA) execution of AT and FP responsibilities listed in DODD 2000.12, "DoD Combating Terrorism Program."

- Promulgate policy and provide oversight to DOD intelligence, counterintelligence, security, and information operations in support of AT and FP intelligence standards.

- Provide appropriate members to the DOD ATCC (and subcommittees as required), the DOD Worldwide AT Conference, and an observer to the OSPG.

e. **The Assistant Secretary of Defense for Force Management Policy (ASD[FMP]),** under the **Under Secretary of Defense for Personnel and Readiness,** shall:

- Provide a member to the DOD ATCC (and subcommittees as required), and a representative to the DOD Worldwide AT conference.

- Establish an AT and/or FP program for the Department of Defense Dependent Schools System.

- In coordination with Service Secretaries, commanders of the combatant commands with geographic responsibility, and the Chairman of the Joint Chiefs of Staff, address AT and FP considerations in establishing tour lengths and determine whether restrictions should be placed on accompanying family members for personnel assigned to overseas activities.

- With the USDA&T, establish policy for inclusion in the Defense Federal Acquisition Regulation to require that Defense contractors who operate overseas or whose employees travel overseas shall:

  •• If the contractors are US companies, affiliate with the Overseas Security Advisory Committee;

  •• Ensure their personnel who are US nationals register with the US embassy and third country nationals comply with the requirements of the embassy of their nationality;

  •• Prior to their travel outside the United States, provide AT and FP awareness information to personnel commensurate with that which the Department of Defense provides to the military, DOD civilian personnel, and their families to the extent such information can be made available; and

  •• Receive the most current AT and FP guidance for personnel, and comply with the Foreign Clearance Guide (FCG), as appropriate.

f. **The ASD(SO/LIC)** shall:

- Serve as ATCC - Senior Steering Group co-chair.

- Provide a Deputy Assistant Secretary-level co-chair for the ATCC.

- Monitor programs to reduce the vulnerability of DOD personnel and their family members, facilities, and other

DOD material resources to terrorist attack with the Chairman of the Joint Chiefs of Staff and other DOD components.

- Ensure compliance with DODD 2000.12, "DoD Combating Terrorism Program," by having all DOD activities (other than combatant commands) report directly to the Secretary of Defense.

- Provide an Office of the Secretary of Defense (OSD) representative to the Interagency Working Group on Terrorism and an observer to the OSPG.

- Provide membership on ATCC subcommittees, as required.

- Provide policy oversight and guidance to the DOD components in support of respective counterterrorism program efforts and work in conjunction with command, control, communications, and intelligence on matters pertaining to other combatting terrorism program elements.

- Develop, publish, and maintain DODD O-2000.12-H, "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence," and DODD 5025.1-M, "DoD Directives System Procedures," consistent with Public Law 99-399, "Omnibus Diplomatic Security and Antiterrorism Act of 1986," to provide standards and guidance on protective measures that serve to reduce the vulnerability of DOD personnel and their family members to terrorist acts.

- Sponsor the DOD Worldwide AT and FP Conference.

- Coordinate DOD combatting terrorism program issues before the DOD Physical Security Review Board, the DOD Physical Security Equipment Steering Group, and other relevant security boards and committees.

- Coordinate with the USDA&T on AT and FP technology development and the application of new technology to meet AT and FP needs.

- Coordinate on Combatting Terrorism Readiness Initiative Fund (CTRIF) requests.

- Identify DOD-designated high and potential physical threat countries in support of DOD travel security policy and issue the TSA message in coordination with the Assistant Secretary of Defense (International Security Affairs), and the Assistant Secretary of Defense (International Security Policy), as appropriate.

g. **The Secretaries of the Military Departments** shall:

- Institute combatting terrorism programs and support them with adequate programming, planning, and funding.

- Incorporate AT and FP into Service doctrine.

- Institute AT and FP training programs in accordance with DODD O-2000.12-H, "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence." Ensure that AT and FP and information on current security technology is incorporated in appropriate Service schools and training commensurate with the level of responsibility or command for which the school is designed.

- Provide AT resident training to personnel assigned to high-risk billets and others, as appropriate.

- Provide prompt dissemination of intelligence information on terrorist threats, including specific warning of threats against DOD personnel and their family members, facilities, and other DOD material resources, in accordance with DODD 5240.1, "DoD Intelligence Activities," DODD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," and DODD 5240.6, "Counterintelligence Awareness and Briefing Program."

- In coordination with the Chairman of the Joint Chiefs of Staff, commanders of the combatant commands with geographic responsibility, and the ASD(FMP), address AT and FP considerations in recommending tour lengths and determine whether restrictions should be placed on accompanying family members for personnel assigned to overseas activities.

- Ensure that current AT and FP technology is incorporated into all acquisition of new facilities, systems, and equipment, where appropriate.

- Establish military construction programming policies to ensure that AT and FP protective features for facilities and installations are included in the planning, design, and execution of military and minor construction projects.

- Ensure that all Service installations and activities are assessed in accordance with (IAW) DODD O-2000.12-H, "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence." Ensure that installations develop, maintain, and implement AT and FP Service-specific standards in concert with Service, commander of a combatant command (CINC), and DOD standards as appropriate.

- Identify the resources programmed to implement and maintain AT and FP for the Services as part of the PPBS process.

- Ensure that Service personnel and their family members comply with the DOD FCG. Ensure that personnel are aware of any TSAs in effect at the time of travel. Ensure that all DOD personnel and family members scheduled for permanent change of station to foreign countries receive appropriate and required training in accordance with DODD O-2000.12-H, "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence."

- Ensure that existing physical security, base defense, and law enforcement programs address terrorism as a potential threat to Service personnel and their family members, facilities, and other DOD material resources.

- Provide a Military Service representative as a member to the DOD ATCC (and subcommittees as required), and a representative to the DOD Worldwide AT Conference.

- Ensure that Service component capabilities exist to collect, receive, evaluate, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack.

h. **The Chairman of the Joint Chiefs of Staff** shall:

- Serve as the principal advisor to the Secretary of Defense for all DOD AT and FP issues.

- Prepare joint doctrine and assist the ASD(SO/LIC) in development and maintenance of AT and FP standards. Review Service doctrine and CINC and

Service standards. Review, coordinate, and oversee (on behalf of the Secretary of Defense and in conjunction with the DOD components) AT and FP training for all DOD personnel and their family members.

- Direct the Joint Requirements Oversight Council (JROC) to address AT and FP requirements. Include in the Chairman's program review and the Chairman's program analysis a summary of AT and FP requirements, determined by the JROC and derived in the CINC-integrated priority lists.

- Assess AT and FP as an element of any force deployment decision. Periodically reassess AT and FP of deployed forces.

- Assess with the DOD components their policies and programs for the protection of DOD personnel, their families, facilities, and other material DOD resources in compliance with DODD 2000.12, "DoD Combating Terrorism Program," and IAW DODD O-2000.12-H, "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence."

- Annually (as part of the budget cycle) review the adequacy of resources proposed by the Services to determine whether they meet DOD AT and FP objectives. Advise the Secretary of Defense of any changes that are needed to meet AT and FP requirements.

- In coordination with the Service Secretaries, the ASD(FMP), and the combatant commanders, address AT and FP considerations and recommend appropriate tour lengths. Advise the Secretary of Defense as to whether restrictions should be placed on accompanying family members for personnel assigned to overseas activities.

- Review the impact of DODD 2000.12, "DoD Combating Terrorism Program," on the Unified Command Plan, issued by the President, and the Secretary's "Forces for Unified Commands" Memorandum (current edition). Recommend revisions to these plans or DODD 2000.12, "DoD Combating Terrorism Program," as required.

- Assess the implementation of terrorist threat conditions (THREATCONs) for uniform implementation and dissemination as specified by DODD O-2000.12-H, "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence," DODD 5025.1-M, "DoD Directives System Procedures," and DODD 2000.12, "DoD Combating Terrorism Program."

- Provide flag and/or general officers as co-chairs for the ATCC Senior Steering Group and ATCC, and provide representatives to the Interagency Working Group on Terrorism, the DOD Worldwide AT Conference, and an observer to the OSPG.

- Coordinate with ASD(C3I) and ASD(SO/LIC) on sharing of terrorism intelligence and counterintelligence data and information on AT and FP. This includes threats posed to DOD personnel and assets by domestic and foreign terrorists.

- Assess the Services', CINCs', and Defense intelligence organizations' capability to collect, evaluate, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack.

- Manage and administer the DOD CTRIF.

- Review the CINCs' information operations and psychological operations (PSYOP) programs for antiterrorism content.

i. **CINCs with geographic responsibilities** shall:

- Establish command policies and a combatting terrorism program for the protection of all assigned forces and for those DOD elements and personnel under the FP responsibility of the CINC as established by MOU. This includes family members, resources, and facilities. This program shall include specific prescriptive standards derived from DODD O-2000.12-H, "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence," that address various geographic settings and specific terrorist threat capabilities.

- Assess and review all CINC-assigned military forces and/or activities within, and DOD forces and/or activities deployed into, their geographic areas of responsibility (AOR), including DOD field activities and agencies that conclude contracts within their AOR and not under the security responsibility of the DOS. This review may be conducted by Service component commands or other subordinate commands reporting to the CINC. Relocate forces as necessary and report pertinent actions taken for FP to the Secretary of Defense via the Chairman of the Joint Chiefs of Staff.

- Coordinate with the Department of State Chiefs of Mission (COMs) in the AOR to ensure security of all non-CINC assigned forces by way of an MOU as necessary.

- Provide updates to the DOD FCG stating command travel requirements and theater entry requirements.

- Provide AT and FP training in accordance with DODD O-2000.12-H, "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence." Ensure that: personnel traveling comply with the FCG; personnel are aware of any TSAs in effect at the time of travel; and all DOD personnel and family members scheduled for permanent change of station to foreign countries receive appropriate and required training IAW DODD O-2000.12-H, "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence."

- In coordination with Service Secretaries, ASD(FMP), and the Chairman of the Joint Chiefs of Staff, address AT and FP considerations in establishing tour lengths and determine whether restrictions should be placed on accompanying family members for personnel assigned to overseas activities.

- In accordance with PPBS procedures, identify the requirements necessary to achieve the AT and/or FP for each activity under the CINC's combatant command (command authority) or for which the CINC otherwise has AT and/or FP responsibility. These requirements will be identified in such a way as to permit their identification as the AT and/or FP resource requirements.

- Establish command relationships and policies for each subordinate command to ensure effective mechanisms are in place to protect and defend against terrorist attack. For JTFs, report to the Secretary of Defense via the Chairman of the Joint Chiefs of Staff any decision to vest operational control for AT and

FP matters outside the JTF commander, and detail the reasons for the decision. Periodically, as directed by the Chairman of the Joint Chiefs of Staff, reassess the appropriateness of command relationships of existing JTFs to ensure that adequate AT and FP measures are in place.

- Identify and disseminate to the force providers specific area pre-deployment training requirements that all personnel must complete prior to arrival in theater. Provide training requirements to Services and agencies for all DOD personnel and family members scheduled for permanent change of station to the theater. Ensure that all personnel assigned to the headquarters receive appropriate AT and FP training.

- Assess the terrorist threat for the theater according to DODD 2000.12, "DoD Combating Terrorism Program," and provide threat assessment information to the Service components and Defense agencies in theater. On the basis of the threat assessment, identify and recommend to the appropriate authority those incumbents of high-risk billets and spouses requiring AT resident training.

- Keep subordinate commanders and COMs informed of the nature and degree of the threat. Ensure that commanders are prepared to respond to threat changes.

- Ensure that AT and FP countermeasures are coordinated with host-country agencies at all levels. Ensure that the COMs are fully and currently informed of any liaison activities relating to the security of those DOD elements and personnel under the security responsibility, but not the command, of the CINC.

- Assist DOD elements, within their geographic regions, in implementing programs developed under DODD 2000.12, "DoD Combating Terrorism Program."

- Ensure that THREATCONs are uniformly implemented and disseminated as specified by DODD 2000.12, "DoD Combating Terrorism Program," DODD 5025.1-M, DoD Directives System Procedures," and DODD O-2000.12-H, "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence."

- Within the theater, through the United States Defense Representatives and COMs, serve as the DOD point of contact with host-nation officials on matters involving AT and FP policies and measures.

- Provide a representative to the DOD ATCC (and subcommittees, as required) and to the DOD Worldwide AT Conference.

- Ensure that a capability exists to collect, evaluate, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack.

- For unanticipated emergency AT and FP requirements that Services cannot fund, forward requirements for submission to the CJCS CTRIF.

- Use information operations and PSYOP to support antiterrorism programs.

j. **CINCs with functional responsibilities** shall:

- Establish command policies and a combatting terrorism program for the protection of all assigned forces. This includes family members, facilities, and other material resources. Coordinate this program with the appropriate CINC for

the geographic area. The geographic CINCs' programs shall take precedence when a conflict in policy or programs exist.

- Ensure all facilities are assessed in coordination with the geographic CINCs and Services in accordance with DODD O-2000.12-H, "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence."

- Ensure that all personnel assigned to the headquarters receive appropriate AT and/or FP training.

- For unanticipated emergency AT and/or FP requirements that Services cannot fund, ensure subordinate commands forward requirements for potential submission to the CJCS CTRIF.

k. **Directors of other Defense Agencies and Field Activities, OSD Principal Staff Assistants, and those that report directly to the Secretary or Deputy Secretary of Defense**, shall:

- Utilize DODD O-2000.12-H, "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence," and DODD 5025.1-M, "DoD Directives System Procedures," for the AT and FP planning and execution for their headquarters and all activities under their cognizance: Consider mission, characteristics of the activity, geographic location, and threat condition. Establish prescriptive standards for installations and facilities not located on Service installations. As appropriate, coordinate with the applicable CINC or Service.

- Ensure that all assigned personnel comply with the DOD FCG. Ensure that personnel are aware of any TSAs in effect at the time of travel. Ensure that all DOD personnel and family members scheduled for permanent change of station to foreign countries receive appropriate and required training in accordance with DODD O-2000.12-H, "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence."

- Provide members to the DOD ATCC (and subcommittees as required), and representatives to the DOD Worldwide AT Conference.

- Identify to the Secretary of Defense, with an information copy to the Chairman of the Joint Chiefs of Staff, the resources required to implement and maintain AT and FP for their respective offices and personnel.

COMBATTING TERRORISM

From the beginning of Operation DESERT SHIELD, the United States was concerned about possible terrorist attack. Consultations and exchanges of information among Coalition partners and other members of the UN led to the expulsion of over 200 Iraqi diplomatic personnel, embassy staff, and intelligence personnel from their posts throughout the world. This undoubtedly had a disruptive effort on Iraqi terrorist operations.

Within the US Government, the National Security Council took the lead in producing a well-founded, coordinated policy. Throughout the conflict the Office of the Secretary of Defense met frequently in the interagency arena to consult and formulate policy options, including employment of special operations forces. These policy determinations involved both components of combatting terrorism: antiterrorism, which involves defensive measures to reduce vulnerability or individuals and property to terrorist acts; and counterterrorism, which involves offensive measures taken to prevent, deter, and respond to terrorism.

SOURCE: Final Report to Congress, Conduct of the Persian Gulf War, April 1992

Intentionally Blank

CHAPTER II
TERRORIST THREAT

"This country swarms with vile outrageous men / That live by rapine and by lawless spoil."

Christopher Marlowe
Tamburlaine the Great, ii, 2, 1587

1. Overview

A critical factor in understanding terrorism is the importance of the emotional impact of the terrorist act on an audience other than the victim. This chapter provides background information concerning the terrorist threat to enable the commander at any echelon to create and employ AT tactics, techniques, and procedures outlined in this publication. **Terrorism has become a media event and, as such, a phenomenon of our time.** The terrorist of today will exploit information operations against the United States as much as the media will allow. News media coverage is important to terrorists who are attempting to incite public fear or gain attention for their cause. Another determinant of tactics and target selection is the role the terrorist group perceives itself as playing. Terrorism can also be used as either an overt or a covert aspect of a political movement engaged in a power struggle within an existing political system. Terrorists frequently claim affiliation with causes or political organizations to give their actions a claim to respectability. Operations to meet the threat may fall in both the CT and AT arenas.

2. Terrorist Tactics

Terrorist tactics vary in sophistication according to the level of training the individual or group has received. Categories of training are trained (entire group has had formal training), semi-trained (a few members have been trained and have passed that training on to the rest of the group), and untrained (no members have had formal training).

Examples of objectives with which a terrorist attack may be associated, but not limited to, are shown in Figure II-1. Just as a terrorist incident may have several objectives, the tactics used may also be combined. **The more common tactics employed by contemporary terrorist groups are listed in Figure II-2 and discussed below.**

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

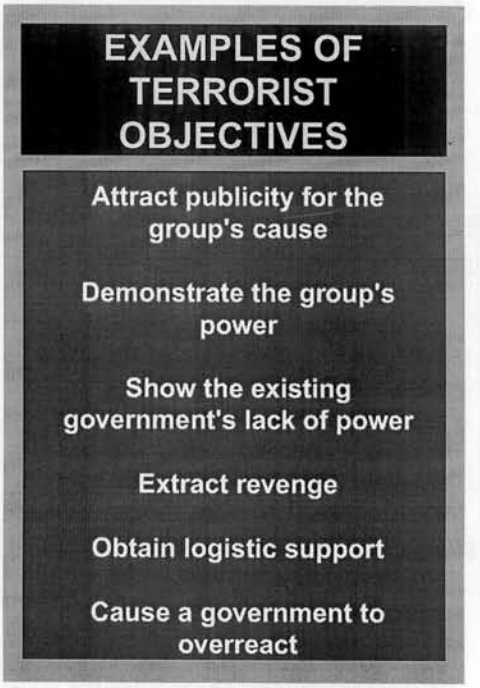


Figure II-1. Examples of Terrorist Objectives



Figure II-2. Common 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.

c. **Bombing. The improvised explosive device (IED) is the terrorist's weapon of choice.** IEDs can be inexpensive to produce and, because of the various detonation techniques available, may be a low risk to the perpetrator. (However, suicidal bombing cannot be overlooked as an employment method.) Other advantages include their attention-getting capacity and the ability to control casualties through time of detonation and placement of the device. It is also easily deniable should the action produce undesirable results. From 1983 through 1996, approximately half of all recorded terrorist incidents worldwide involved the use of explosives.

d. **Hostage Taking.** This usually is **an overt seizure of one or more individuals with the intent of gaining publicity or other concessions in return for release of the hostage**. While dramatic, hostage and hostage barricade situations are risky for the perpetrator.

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

f. **Hijacking or Skyjacking.** Sometimes employed as a means for escape, **hijacking is normally carried out to produce a spectacular hostage situation**. Although trains, buses, and ships have been hijacked, aircraft are the preferred target because of their greater mobility and vulnerability.

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

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



Port facilities are particularly vulnerable to terrorist sabotage.

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

j. **Hoaxes. Any terrorist group that has established credibility can employ a hoax with considerable success.** A threat against a person's life causes that person and those associated with that individual to devote time and effort to security measures. A bomb threat can close a commercial building, empty a theater, or delay an aircraft flight at no cost to the terrorist. False alarms dull the analytical and operational efficiency of key security personnel, thus degrading readiness.

k. **Use of Special Weapons.** Chemical weapons have been used by terrorists to date and there is potential for the use of both chemical and biological weapons in the future. These types of weapons, relatively cheap and easy to make, could be used in place of conventional explosives in many situations. **The potential for mass destruction and the deep-seated fear most people have of chemical and biological weapons could be attractive to a group wishing to make the world take notice.** Although an explosive nuclear device is acknowledged to be beyond the reach of most terrorist groups, a chemical or biological weapon or a radiological dispersion device using nuclear contaminants is not. The technology is simple and the cost per casualty (for biological weapons in particular) is extremely low — much lower than for conventional or nuclear explosives. This situation could change as the competition for headlines increases.

l. **Environmental Destruction.** Although this tactic has not been widely used, **the increasing accessibility of sophisticated weapons and explosives to terrorists has the potential to threaten damage to the environment.** Examples would be intentional dumping of hazardous chemicals into a city's water supply or the destruction of an oil tanker.

m. **Use of Technology.** Technology has important implications for the terrorist threat faced by DOD personnel. Infrastructure technologies provide attractive targets for terrorists who can apply a range of rudimentary and advanced attack techniques to disrupt or undermine confidence in a range of systems. Key elements of the national infrastructure, such as transportation, telecommunications, energy, banking, public health, and water supply are becoming increasingly dependent on computerized systems and linkages.

- These systems provide targeting opportunities for adversaries who possess even limited technological capabilities, and who have the ability to identify critical system choke points. Terrorists can apply computer generated attacks or more traditional means such as bombs or physical destruction to cause system-wide malfunctions. Interdependencies of systems, such as power and transportation, exacerbate this vulnerability. Significant disruption of power grids can have a devastating impact on air traffic control, railway operations, port operations, and emergency services such as fire and/or rescue and police. Attacks such as power outages also impact a wide segment of the population, command significant media attention and consequently provide an effective means for the terrorist to reach a "captive" audience.

- A range of technologies can also be employed effectively by terrorists to conduct operations. Although terrorists to date have not demonstrated significant technological innovation and have largely relied on traditional attack methods such as bombing, hostage taking, and assaults, several factors point to an increased likelihood of greater use of more sophisticated technologies. First, the wide scale proliferation of military weapons and technologies that has followed the collapse of the former Soviet Union has increased the range of weapons available on international arms markets. Stand-off weapons such as shoulder-fired anti-aircraft weapons, light anti-tank weapons which have been used in attacks against US targets in the past, are attractive means of attack for a terrorist since they reduce vulnerability and increase chance of escape. Increased availability of more powerful explosives (such as the plastic explosive Semtex, which is easily concealed and difficult to detect), when combined with more sophisticated timing devices, detonators, and fuses, have provided the terrorist with much more lethal bombing capabilities.

- Increasing availability of nuclear, biological, and chemical (NBC) material, components, and weapons raises the specter of terrorists using these weapons in an attack against civilian populations or military facilities. The 1995 Tokyo subway Sarin nerve gas attack by the Aum Shinrikyo cult, resulting in the death of 12 and injury of 5,500 people, is the most vivid example of the threat from NBC weapons. Many chemical-biological (C-B) weapons ingredients are commercially available, and there are numerous reports throughout Europe of fissile material availability on the black market. This raises the possibility not only of terrorist use of nuclear weapons, but of radiological bombs that use fissile material to contaminate targets.

- A range of commercially available technologies can dramatically enhance terrorist operational capability. These include communications equipment, encryption capabilities, surveillance equipment, weapons, a range of computer and information management technologies, weapons components, and the Internet. The ability to acquire or

adapt technologies can give terrorists an edge in choosing targets and conducting attacks as well as significantly expanding their range of attack options.

- Technological advances also enhance antiterrorism capabilities. Recent research and development efforts have focused on the following areas:

  •• detection of explosives and other weapons;

  •• detection of, and defense against, C-B agents;

  •• physical protection (e.g., alarms, barriers, access control);

  •• incident response; and

  •• data analysis and dissemination.

- Explosive detection technologies can be applied for both airline security and for fixed facilities. They detect physical, chemical, or mechanical properties of bombs using a variety of technologies, from x-rays and radio waves to dogs and "sniffer" technologies.

- Detection of C-B agents poses a significant challenge, since almost anyone that can brew beer can manufacture a biological agent, and toxic chemicals are widely available on the commercial market. Laser technologies have shown promise in detection of C-B agents, and research and development work on personnel protective equipment and vaccines is being pursued aggressively.

- A range of technologies is currently being investigated to enhance physical protection capabilities. Access control technologies, which include a range of personnel identification systems, metal detectors, and closed circuit surveillance devices are being researched and fielded on a regular basis. Barrier technologies are also being fielded, and enhancements in building design to enhance bomb resistance are being incorporated into new and existing DOD buildings in high threat areas.

- Incident response technologies are developed to assist in responding to assaults on facilities, hostage taking, or criminal activities. Incident response activities include disrupting the attack, defending targets, aiding persons injured in an attack, rescuing hostages, and apprehending attackers. A broad range of technologies are included in this category such as fiber-optic and low-light camera technologies, highly accurate sensors, nonlethal weapons, incapacitating agents, and software tools for profiling terrorists and supporting response planning.

- Effective data dissemination is a key measure to improving antiterrorism awareness and preparedness. The rapid evolution of information technology has facilitated the transfer of accurate terrorist profiles (to include photographs) and the ability to transfer the information anywhere in the world quickly. Other key AT data, such as protection technologies and procedures, can also be transmitted to field locations quickly and effectively. Recent efforts have reduced barriers between agencies on the fusion and dissemination of AT data.

3. Terrorist Groups

A terrorist group's selection of targets and tactics is also a function of the group's affiliation, level of training, organization, and sophistication. For several years, **security forces categorized terrorist groups according to their operational traditions—**

national, transnational, and international. National groups operated within the boundaries of a single nation. Transnational groups operated across international borders. International groups operated in two or more nations and were usually assumed to receive direction and support from a foreign government. **Terrorist groups are categorized by government affiliation** to help security planners anticipate terrorist targets and their sophistication of intelligence and weaponry. Three general terrorism categories are shown in Figure II-3.

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. Messianic 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 the Abdul-Ramman group that perpetrated the World Trade Center bombing), "state-supported" (e.g., extremist factions of HAMAS who believe violence serves their concept of religious servitude), or "state-directed" (e.g., Hizballah is both the "Party of God" and a religious cult organization that employs violence in support of both religion and politics).



Figure II-3. Categories of Terrorist Groups

4. Terrorist Organization

As with any organization, terrorist groups develop organizational structures that are functional for the environment in which they operate. Because terrorists usually operate in a hostile environment, **security is the primary consideration**. As a result, **the organization of terrorist groups is usually cellular, with each cell relatively isolated and performing specific functions such as intelligence gathering or logistic operations**. This type of organization protects members of the group. In the event of defection or capture, no one member can identify more than a few of the others. Some groups have multifunctional cells that combine several skills in one operational entity, while others create cells of specialists that come together for an operation on an ad hoc basis. The latter procedure is similar to tailoring or task organizing military forces.

a. **Larger terrorist groups (100 or more members) normally have a central command and control element with one or more subordinate elements** based on geographical regions. The regional commands direct the actions of the operational and support cells in their region. **Smaller groups (50 or fewer members) may have a single command element** that directly controls all of the operational and support cells regardless of where they are established.

b. **Terrorist groups often structure themselves in a manner similar to military organizations**, but groups vary as to the degree of discipline and lines of authority and

function. Such organizations have historically had well-defined, organized structures that made penetration difficult. In other instances, group dynamics, egos, and philosophical differences override organizational principles and create opportunities for security forces to identify members, penetrate the organization, and/or prevent terrorist actions. These **personal factors often cause such terrorist groups to splinter into new faction(s)** (e.g., Popular Front for the Liberation of Palestine, Popular Front for the Liberation of Palestine-General Command, and Democratic Front for the Liberation of Palestine), adding to the growing list of organizational titles in world terrorism. Along with the commonly used deception technique of claiming credit for an action in the name of a previously unknown group, **splintering complicates security force intelligence efforts and creates confusion in determining the decision makers**, thus making the organizations generally hard to break.

c. In a broader context, **terrorist organizations**, especially those with little or no access to government resources, **need a support structure**. As shown in Figure II-4, a typical organization consists of operational members who are functionally organized as outlined above and have several categories of supporters.

- **At the top is the leadership** that defines policy and directs action. Typically, leaders are completely committed to the cause that the group purports to serve and may be charismatic figures. If the group is state-supported or state-directed, the leadership will include one or more members who have had extensive training or education by the sponsoring state.
- **The active, operational cadre are the doers** — the men and women who carry out terrorist attacks and train others. As

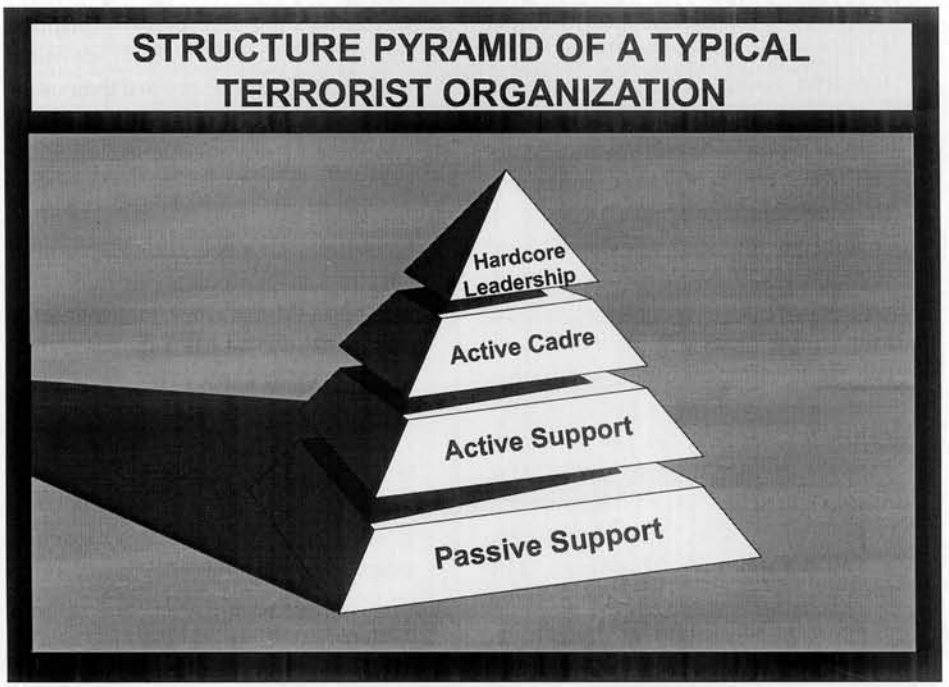


Figure II-4. Structure Pyramid of a Typical Terrorist Organization

in the planning and leadership elements, many doers are deeply committed to the group's cause. The professionals who may or may not be ideologically motivated are also part of the active cadre.

- **Active supporters do not actually commit violent acts but assist the terrorists by providing money, intelligence, legal or medical services, and/or safe houses or forged documents.** This includes supporters both within the country and in other countries. Active supporters are frequently ideologically in agreement with all or some of the terrorist group's goals but may be ambivalent concerning the use of violence. Terrorist groups recruit most of their cadre from the ranks of the active supporters because those people have proven their loyalty and, to some extent, their skills over a period of time.

- **Passive supporters are the most difficult to define** and identify. **Most of these people are sympathetic to the terrorist group's cause**, but will not assume an active role due to fear of reprisal if exposed or identified. Family and acquaintances of activists sometimes fall into this category, especially in cultural environments where family and regional loyalties are strong. Often, passive supporters are not sympathetic to the terrorist cause but do not believe that the government can or will protect them. Thus, fear rather than sympathy generates support for the terrorist. Passive supporters may be ignorant to the cause's intent and use of their support; consequently, they may unwittingly provide anonymous funding. The terrorist group relies on passive supporters for financial assistance, displays of public support, and minor logistic or operational tasks. Passive support is extremely important to the politically-motivated terrorist who relies on popular support to survive.

d. Membership in terrorist organizations brings together people who commit terrorist acts for different motivations. **Not all terrorists are committed to their cause by ideology.** Many terrorist groups are augmented by criminals (professionals) who are opportunists seeking personal rather than political gain or by individuals who are mentally disturbed. **Many individuals responsible for terrorist acts could fit into one of three categories; crusaders, criminals, or emotionally disturbed.** Although the criminal or emotionally disturbed person may not fit the strict definition of a terrorist, the varied motivations and ambiguities of terrorism necessitate their inclusion in the same context with the crusader. A specific individual may exhibit traits from more than one category. Terrorists look like ordinary citizens and come from all walks of life.

- **Crusaders** are ideologically inspired individuals or groups (e.g., political terrorists). They believe that their cause is so noble or worthy that it may be promoted by any means, including the use of terror.

- **Criminals or professionals** commit terrorist acts for personal gain rather than ideology. Although they often mimic the crusader's ideological conviction, their devotion to the cause is not the primary motivation. Crusaders often recruit criminals for their knowledge, background, and criminal skills.

- **Emotionally or mentally disturbed people** who commit terrorist acts often believe that they have some special mandate from a deity. They can range in character from compulsive, minute planners to impulsive, unpredictable doers. Additionally, emotionally

disturbed people often obtain some level of enjoyment in the terrorist act. The emotionally and mentally disturbed are often used by terrorist organizations as throwaway or disposable terrorists. They usually drive the truck bomb or become martyrs for a cause.

5. Terrorist Targets — Americans

It is sometimes difficult for Americans to understand why **terrorism seems to thrive in the environment that offers the least justification for political violence** (e.g., democracies and ineffective authoritarian regimes). Equally puzzling is the relative absence of terrorism in those societies with totalitarian and effective authoritarian governments. The reasons for this apparent paradox can be summarized as being a matter of social control. The terrorist operates covertly. **In societies where little is done without the knowledge of internal security agencies, covert activity for any appreciable period of time is difficult.** The same principle applies to acquisition of weapons, communications equipment, and explosives. Another factor is public information. Because the terrorist's objectives usually include gaining the attention of a target audience through a violent act, the terrorist can easily be denied that objective in an environment where information media are tightly controlled. Finally, in controlled societies, the ability of terrorist organizations to create functional networks or to move funds within the financial system are severely hindered.

a. The reasons US interests are a target for so many terrorist groups around the world are complex and must be understood in order to effectively combat terrorism in the long term. **One reason some terrorist groups target the United States and its citizens is ideological differences.** The United States is a leading industrial power and the leading capitalist state. These reasons are enough to incite the animosity of some groups that are committed to different social systems.

b. **Of greater importance is the perception that the US Government can dictate courses of action to other governments.** Terrorists think that by pressuring the United States through acts of terror, the US Government will bring pressure to bear on the targeted government to comply with terrorists' demands. Although US influence is substantial in the world community, this is not a policy of the US Government.

c. **Mere presence is another factor.** Americans are all over the world in capacities ranging from diplomatic service to tourists. This availability makes targeting Americans easy even for relatively poorly trained non-state-supported groups. It also adds to the chances of Americans being killed or injured



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

unintentionally. These same considerations apply to members of the US military forces with the added factor of "symbolic value." The Armed Forces are clearly visible symbols of US projection of power and presence; thus, terrorists find military personnel and installations appealing targets.

6. Domestic Terrorism

a. Despite recent bombings in New York, Oklahoma, and Atlanta, the United States has a low rate of terrorism compared to Europe, Latin America, Africa, or the Middle East. **A tradition of violence for political purposes has not been a dominating means of achieving political power.** There is no history of deep ideological commitment justifying the taking or sacrificing of life. Although there have been limited exceptions to this observation — such as some Puerto Rican independence groups — they have not gained political acceptance at the national level. The relatively open US political system allows minority groups to voice concerns legitimately through the political process. Recently, however, groups of domestic separatists have targeted federal institutions for violence. These attacks indicate a growing willingness to attack symbols of the US Government, despite the relatively open US political system which allows minority groups to voice concerns legitimately through the political process.

b. Caution must be exercised in drawing conclusions exclusively from past experiences. **Although low levels of domestic terrorism have occurred in the United States to date, terrorism is still a threat here.** Radicals and religious extremist organizations and the rise of militias constitute a growing threat to public order. Racial supremacists as well as the violent fringe of environmental and antiabortion movements have also attempted to use terrorism. Agents of external causes and foreign powers pose a potential threat that needs only a transoceanic flight or border crossing to become active. Additionally, computer hackers anywhere in the world can send viruses via the Internet.

7. Terrorism Against the US Military

a. **Terrorism is a major factor across the range of military operations.** In the context of peacetime military operations, terrorism attracts a great deal of attention and few question its actual and potential capacity to kill and destroy. The same can be said of terrorism as an aspect of military operations other than war (MOOTW); however, in war the threat of terrorism is only one of many FP issues the commander must consider. The same types of acts that gain attention in peacetime military operations can hinder military operations in war (e.g., espionage, sabotage, vandalism, or theft).

TERRORISTS AND TOURISM

The most effective fear that the terrorist can generate for the tourist is that he will never arrive at his destination — or will never return home alive. Convinced of this, a supply of tourist visitors could suddenly dry up. Expensive tourist infrastructures, depending on a constant flow of customers — margins in the tourist industry are often surprisingly slender — then lie idle. The industry is very labor intensive so a considerable unemployment problem is created . . . A pistol pointed at a hostage in an aircraft, then, could be a pistol pointed at a country's economic heart.

SOURCE: G. Norton, quoted in Chris Ryan, Tourism, Terrorism and Violence Research Institute for the Study of Conflict and Terrorism, September 1991

b. **All acts of violence against the US military are not necessarily terrorist actions** (e.g., murder or robbery). The measures contained within this publication provide guidance that will help protect the military unit and Service member from these acts of violence as well as those committed by terrorists. In peacetime military operations, there is no definitive method of differentiating terrorist acts from other violent crimes because the perpetrator's intent may be the only discriminator. A rule of thumb that can be applied is if the act is obviously related to personal gain (robbery of money or high-value items) or personal motivation (hatred, love, revenge) it is a crime, but probably not terrorist-related. On the other hand, **if the act appears to adversely affect military operations** (communications facilities, fuel storage areas) **or has a high symbolic value** (headquarters, particular individuals), **the crime probably has terrorist implications even when no claim is forthcoming**. Recognizing the difference between acts of violence and terrorist acts is vital in order to properly understand the threat's intent and determine required defensive measures.

Intentionally Blank

CHAPTER III
LEGAL CONSIDERATIONS

"US forces will act unilaterally and in concert with security partners, using all means authorized by the President and the Congress to counter international terrorism at home and abroad."

National Military Strategy of the United States of America, 1997

1. General

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

2. US Policy

Over the last decade, the US Government has developed a policy regarding terrorism that encompasses acts against Americans both at home and abroad. **The policy is summarized as follows.**

a. **All terrorist actions are criminal and intolerable, whatever their motivation, and should be condemned.**

b. **All lawful measures to prevent such acts and to bring to justice those who commit them will be taken.**

c. **No concessions to terrorist extortion will be made,** because to do so will merely invite more terrorist actions.

d. **When Americans are abducted overseas, the United States will look to the host government to exercise its responsibility under international law** to protect all persons within its territories, to include effecting the safe release of hostages.



Joint forces must take lawful measures to prevent terrorist attacks.

The United States has made the services of the Federal Bureau of Investigation (FBI) available to assist in these situations.

e. **Close and continuous contact with host governments will be maintained during an incident.** Intelligence and technical support will be offered to the maximum extent practicable.

f. **International cooperation to combat terrorism remains a fundamental aspect of US policy** because all governments, regardless of structure or philosophy, are vulnerable; all avenues to strengthen such cooperation will be pursued.

3. Lead Agencies

See Figure III-1.

a. **The DOS is the lead agency for response to terrorism outside the United States, other than incidents on US flag vessels in international waters.** The exception to this is on the Arabian Peninsula where the DOS and Department of Defense signed an MOU transferring responsibility for security of forces on the Arabian Peninsula to the Department of Defense.

b. **The DOJ is the lead agency for domestic terrorism; the FBI is the lead**

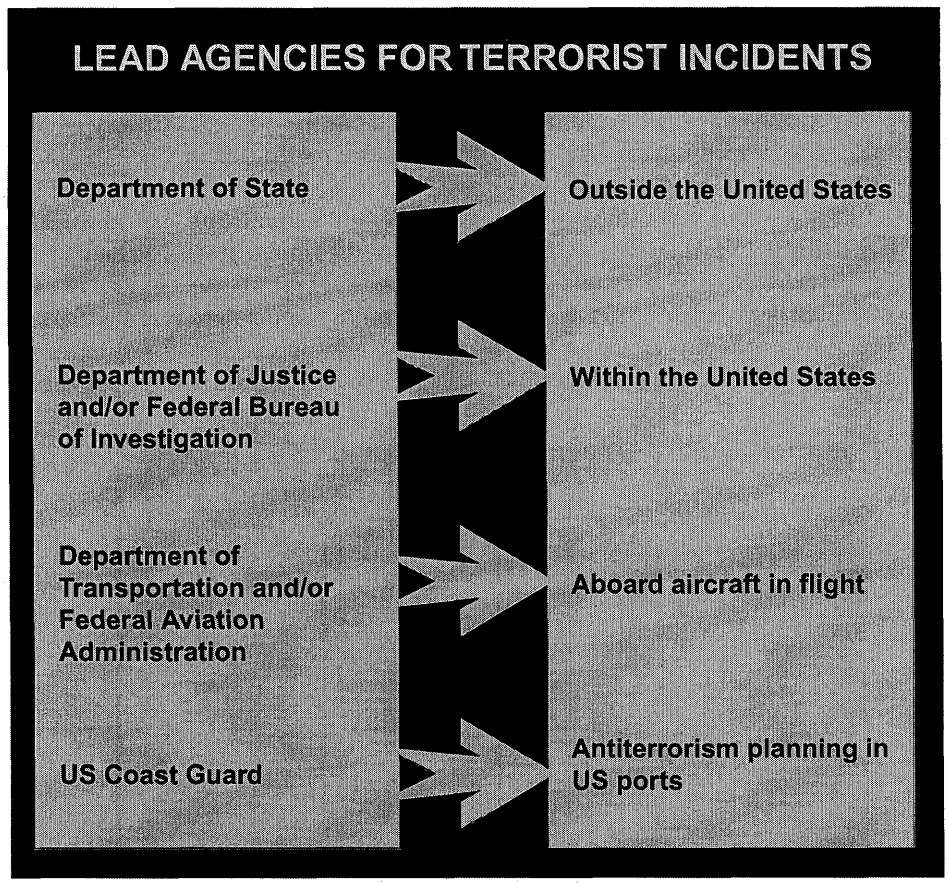


Figure III-1. Lead Agencies for Terrorist Incidents

agency within the DOJ for operational response to terrorist incidents.

c. **The DOT and/or FAA serve as the lead agency for terrorist incidents that occur aboard an aircraft in flight within US jurisdiction.** They are also responsible for investigating and preventing aircraft piracy and for informing commercial air carriers and their passengers regarding any terrorist threat information.

d. By public law, the DOJ (specifically the FBI) is responsible for all search and recovery operations involving nuclear weapons conducted in the United States, District of Columbia, Commonwealth of Puerto Rico, and US possessions and territories, including those conducted on military installations. The DOS is the lead agency for acts not under FBI responsibility.

e. **The US Coast Guard (USCG) is responsible, within the limits of US territorial seas, for reducing the risk of a maritime terrorist incident** by diminishing the vulnerability of ships and facilities through implementation of security measures and procedures. The FBI is the lead agent for responding to terrorist actions that occur in maritime areas subject to US jurisdiction. Further, the USCG is responsible for AT planning in US ports and the implementation of a foreign port assessment program to determine the vulnerability to terrorist attack in certain high and medium risk ports. The USCG is a provider of port security units which can be employed by the CINC as AT and FP assets. The National Terrorism Hotline is manned by the USCG's National Response Center (NRC) 24 hours a day. NRC operators take reports of actual and/or potential domestic terrorism and link emergency calls with the Chemical and Biological Defense Command for technical advice on dealing with weapons of mass destruction (WMD) and with the FBI to initiate the federal response actions. The NRC also provides reports and notifications to other federal agencies as necessary. Additionally, the USCG and FBI have interagency agreements to cooperate with each other when coordinating CT activities and general law enforcement activities. Guidance regarding the USCG's roles can be found in Commandant Instruction 16000.12, "Marine Safety Manual," Volume VII - "Port Security," and Volume X - "Interagency Agreements and Acronyms."

f. All other Federal agencies possessing resources for responding to terrorism are linked together through agency command centers and crisis management groups to ensure effective coordination of the US response.

SECTION A. LEGAL CONSIDERATIONS: AUTHORITY

4. Criminal Actions

Terrorist acts are criminal acts, whether committed during MOOTW or war; however, jurisdiction varies in wartime. **By definition, terrorists do not meet the four requirements necessary for combatant status** (wear uniforms or other distinctive insignia, carry arms openly, be under command of a person responsible for group actions, and conduct their operations in accordance with the laws of war). Only combatants can legitimately attack proper military targets. For this reason, **captured terrorists are not afforded the protection from criminal prosecution attendant to prisoner of war status**. However, Article III of the 1949 Geneva Conventions, which requires that noncombatants be treated in a humane manner, also applies to captured terrorists.

5. Jurisdiction

In peacetime, terrorist acts are normally punishable only under domestic (local) law. However, **in an internationally recognized war or MOOTW involving the use of force (regional or global), terrorists can be tried under local criminal law or under military jurisdiction by either a courts-martial or military tribunal.**

6. Commander's Authority

A commander's authority to enforce security measures and to protect persons and property is paramount during any level of conflict. Commanders must coordinate with their judge advocates to determine the extent of their authority to combat terrorism.

SECTION B. LEGAL CONSIDERATIONS: PERMISSIBLE LIMITS OF MILITARY SUPPORT TO CIVIL AUTHORITIES

7. General

Legal and policy restrictions on the use of active duty DOD military personnel, DOD civilian employees, and contractors such as DOD security police for direct enforcement of civil laws in the United States or its possessions **are contained in the Posse Comitatus Act** (18 USC 1385), **other federal statutes** (10 USC 371-382), **DODDs** (DODD 5525.5, "DoD Cooperation with Civilian Law Enforcement Officials"), and **applicable Service Directives** (such as SECNAVINST 5820.7 series for the Navy and Marine Corps and AFI 10-801 and AFI 10-802 for the Air Force). These laws and policies provide a general prohibition against the use of the uniformed Services of the Department of Defense, either as part of a Posse Comitatus or in a military role other than as provided by statute, to assist local law enforcement officers in carrying out their duties. The same prohibitions apply to the use of troops to execute Federal laws (See 41 Op. Atty. Gen. 330[1957]; 16 Op. Atty. Gen. 162[1878]). **The purpose of this restrictive legislation is to maintain congressional control over the manner and circumstances under which military power could be used in domestic affairs.** Although statutory exceptions allow the use of military forces in some contexts, prior to committing their forces for these purposes commanders shall consult with their judge advocates and refer to applicable DOD and Service Directives, including DODD 3025.1, "Military Support to Civil Authorities (MSCA)," DODD 3025.12, "Military Assistance for Civil Disturbances (MACDIS)," DODD 3015.15, "Military Assistance to Civil Authorities," and DODD 5525.5, "DoD Cooperation with Civilian Law Enforcement Officials." The USCG is also a law enforcement agency. The USCG is authorized to enforce or assist in the enforcement of all Federal laws applicable on, over, and under the high seas and waterways subject to US jurisdiction (14 USC 2).

8. Statutory Authorizations Allowing the Use of the Military

Congress, pursuant to its constitutional authority, has provided a broad range of legislation authorizing the President to use regular and National Guard forces called into federal service to enforce the laws. **To illustrate, the President is currently empowered to use military forces for the following purposes:**

a. **To restore and maintain public order.**

- **To respond to requests for aid from state governments** (10 USC 331). Whenever the President considers that unlawful obstructions, combinations, assemblages, or rebellion against the authority of the United States make it

impracticable to enforce the laws of the United States in a state or territory by the ordinary course of judicial proceedings, Federal armed forces may be used as deemed necessary to enforce those laws or to suppress the rebellion under the statute (10 USC 332).

- **To protect constitutional rights under certain conditions** (10 USC 333). The Fourteenth Amendment to the Constitution forbids any state to deny equal protection of the laws to any person within its jurisdiction. Congress has implemented this provision by providing that a state will be deemed to deny equal protection of the laws if the authorities of the state are unable, fail, or refuse to provide such protection whenever insurrection, civil violence, unlawful combinations, or conspiracies in the state oppose, obstruct, or hinder the execution of state and US laws so that any of the population of the state are deprived of rights, privileges, and immunities named in the Constitution and secured by laws. Thereupon, it becomes the duty of the President to take such measures, by intervention with Federal armed forces or by other means necessary, to suppress such disturbances.

- Whenever the President considers it necessary to use the National Guard or Federal armed forces under the authority of the intervention statutes discussed above, the President must immediately issue a proclamation ordering the insurgents to disperse and retire peaceably to their abodes within a limited time (10 USC 334). If the proclamation is not obeyed, an executive order is then issued directing the Secretary of Defense to employ the Federal military forces necessary to restore law and order. (DODD 3025.12, "Military Assistance for Civil Disturbances [MACDIS]," paragraph V.C.2a, as amended).

- **To protect Federal property and functions** (18 USC 231 and 1361 and 50 USC 797).

b. **To meet specified contingencies.**

- **To assist the US Secret Service in protecting the President, Vice President, major political candidates, and foreign dignitaries** (Section 6 of the Presidential Protection Assistance Act of 1976, Public Law No. 94-524, 90 Stat. 2475 [18 USC 3056 note 1988]).

- **To assist Federal magistrates** in carrying out magisterial orders relating to civil rights violations (42 USC 1989).

- **To assist the Attorney General** in enforcing drug abuse prevention and control (21 USC 873[b]).

- **To assist the administrator of the Environmental Protection Agency** in water pollution control functions (33 USC 1314[k][1]).

- **To assist the FBI** in investigations of congressional assassination, kidnapping, and assault (18 USC 351[g]).

c. **To cope with domestic emergencies and to protect public safety.**

- **Emergency Rule.** When immediate action is necessary to save lives, prevent human suffering or mitigate great property damage and when conditions and time do not permit awaiting prior approval from higher headquarters, a commander may take whatever action the circumstances reasonably justify. However, the commander must comply with the following:

  - Report the military response to higher headquarters;

•• Document all the facts and surrounding circumstances to meet any subsequent challenge of impropriety (i.e., who, what, when, where, how, and why);

•• Retain military response under the military chain of command; and

•• Limit military involvement to the minimum demanded by necessity.

- Emergency situations include, but are not limited to, the following:

  •• Providing civilian or mixed civilian and military firefighting assistance where base fire departments have mutual aid agreements with nearby civilian communities;

  •• Providing emergency explosive ordnance disposal (EOD) service (DODD 3025.15, "Military Assistance to Civil Authorities"; and

  •• Using military working dog (MWD) teams in an emergency to aid in locating lost persons (humanitarian acts) or explosive devices (domestic emergencies).

- To assist the Attorney General in emergency situations involving chemical or biological WMD (10 USC 382, 18 USC 175, and 18 USC 2332c).

SECTION C. LEGAL CONSIDERATIONS: JURISDICTION AND AUTHORITY FOR HANDLING TERRORIST INCIDENTS

9. Jurisdictional Status of Federal Property in the United States, Its Territories, and Its Possessions

In determining whether a Federal or state law is violated, **it is necessary to look not only to the substance of the offense but to where the offense occurs.** In many cases, the location of the offense will determine whether the state or Federal Government will have jurisdiction to investigate and prosecute violations. **There are four categories of Federal territorial jurisdiction: exclusive, concurrent, partial, and proprietorial. These are shown in Figure III-2 and discussed below:**

a. **Exclusive jurisdiction** means that the Federal Government has received, by whatever method, all of the authority of the state, with no reservations made to the state except the right to serve criminal and civil process. In territory that is under the exclusive jurisdiction of the United States, a state has no authority to investigate or prosecute violations of state law. However, the

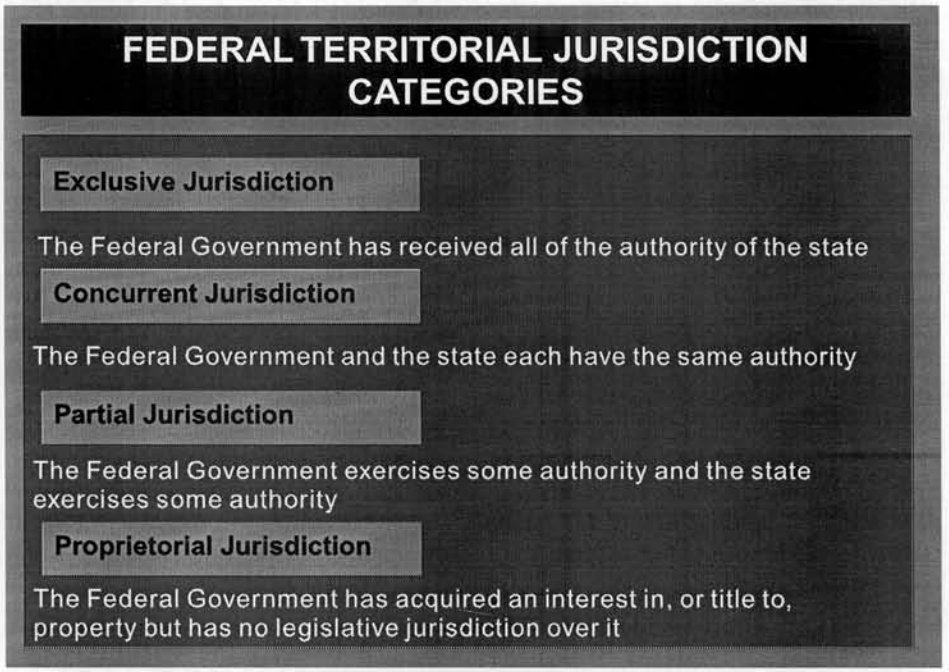


Figure III-2. Federal Territorial Jurisdiction Categories

Assimilative Crimes Act (18 USC 13) allows the Federal Government to investigate and prosecute violations of state law that occur within the special maritime and territorial jurisdiction of the United States.

b. **Concurrent jurisdiction** means that the Federal Government and the state each have the right to exercise the same authority over the land, including the right to prosecute for crimes. In territory that is under the concurrent jurisdiction of the United States and a state, both sovereigns have the authority to investigate or prosecute violations of Federal and state law respectively. In addition, the Federal Government may prosecute violations of state law under the Assimilative Crimes Act.

c. **Partial jurisdiction** refers to territory where the Federal Government exercises some authority, and the state exercises some authority beyond the right to serve criminal and civil processes, usually the right to tax private parties. In territory that is under the partial jurisdiction of the United States, a state has no authority to investigate or prosecute violations of state law, unless that authority is expressly reserved. Unless the state has reserved the right to exercise criminal jurisdiction over the property concerned, the Federal Government may prosecute violations of state law under the Assimilative Crimes Act.

d. **Proprietorial jurisdiction** means that the Federal Government has acquired an interest in or title to property, but has no legislative jurisdiction over it. In territory that is under the proprietary jurisdiction of the United States, the United States has the authority to investigate and prosecute non-territory-based federal offenses committed on such property, such as assault on a federal officer. This authority does not extend to investigations and prosecution of violations of state laws under the Assimilative Crimes Act and Federal Crimes Act of 1970. The

state has the authority to investigate and prosecute violations of state law that occur on such territory.

10. Federal Authority in the United States, Its Territories, and Its Possessions

There are several Federal criminal statutes that may apply to terrorist activities. Some deal with conduct that is peculiar to terrorism, and others prescribe conduct that is criminal for anyone but in which the terrorist may engage to accomplish his or her purposes. **The Federal law contains no special prohibition against terrorist acts or threats, as do some state codes.** However, the Assimilative Crimes Act will allow the Federal Government to investigate and prosecute violations of state law regarding terrorist acts or threats that occur within the exclusive, concurrent, or partial jurisdiction of the United States, thereby giving the Federal Government investigative and prosecutorial jurisdiction over a wide range of criminal acts. Once a violation of Federal law occurs, the investigative and law enforcement resources of the FBI and other Federal enforcement agencies become available, and prosecution for the offense may proceed through the Office of the United States Attorney General.

11. Federal and State Concurrent Authority

In some cases, terrorist acts may be violations of state law as well as Federal law. In this situation, both state and Federal enforcement authorities have power under their respective criminal codes to investigate the offense and to institute criminal proceedings. If a terrorist act is a violation of both Federal and state law, then the Federal Government can either act or defer to the state authorities depending on the nature of the incident and the capabilities of local authorities. Even where the Federal Government defers to state authorities, it can provide law enforcement assistance and support to local authorities on request. **The choice between Federal or state action is made by the prosecuting authority.** However, successive prosecutions are possible even where Federal and state law proscribe essentially the same offense, without contravening the Fifth Amendment prohibition against double jeopardy. Two relevant factors regarding law enforcement responsibility for a given incident are:

a. The capability and willingness of state or Federal authorities to act; and

b. The importance of the state or Federal interest sought to be protected under the criminal statute.

12. Jurisdictional Authority

The matrix in Appendix L, "Jurisdictional Authority for Handling Terrorist Incidents," provides a summary of FBI, host-nation, and commanding officer authority and jurisdiction in investigating or resolving terrorist incidents.

SECTION D. LEGAL CONSIDERATIONS: FEDERAL AGENCIES AND THE MILITARY

13. Overview

The primary Federal organizations dealing with terrorism management are the National Security Council (NSC), DOS, and DOJ.

14. The National Security Council

The NSC assists the President in formulating US policy for dealing with terrorist acts and advises the President on terrorist threats that endanger US interests.

15. The Committee to Combat Acts of Terrorism

This committee was reorganized in 1977 to coordinate, through its working group executive committee, the activities of 31 Federal organizations. **The working group focuses primarily on the protection of foreign diplomatic personnel in the United States as well as American officials working and traveling abroad.** The 31 member agencies, including the Department of Defense, may provide assistance in the form of terrorist incident information, technical assistance about security precautions, public information, and participation in education seminars. Because the DOS has the primary responsibility for dealing with terrorism involving Americans abroad, it chairs this committee. Although a foreign nation has responsibility for responding to incidents occurring on its territory, the Department of Defense or other US agencies may be invited to provide assistance if American interests are involved. In such cases, the US COM oversees the activities of US agencies.

16. Department of Justice

The DOJ is **responsible for overseeing the Federal response to acts of terrorism within the United States.** The US Attorney General, through an appointed Deputy Attorney General, makes major policy decisions and legal judgments related to each terrorist incident as it occurs.

17. Federal Bureau of Investigation

The FBI has been designated **the primary operational agency for the management of terrorist incidents occurring within the United States.** When a terrorist incident occurs, the lead official is generally the special agent in charge (SAC) of the field office nearest the incident and is under the supervision of the Director of the FBI. The FBI maintains liaison with each governor's office. Because of the presence of concurrent jurisdiction in many cases, the FBI cooperates with state and local law enforcement authorities on a continuing basis. In accordance with the Atomic Energy Act of 1954, the FBI is the agency responsible for investigating a threat involving the misuse of a nuclear weapon, special nuclear material, or dangerous radioactive material. In this effort, the FBI cooperates with the Departments of Energy and Defense, the Nuclear Regulatory Commission, and the Environmental Protection Agency as well as several states that have established nuclear threat emergency response plans.

18. Department of Defense

DODD 2000.12, "DoD Combating Terrorism Program" prescribes that **the ASD(SO/LIC) has the lead role within the Department of Defense** in countering domestic terrorist incidents where US forces may be used. However the Attorney General, through the FBI, will remain responsible for coordinating:

- The activities of all Federal agencies assisting in the resolution of the incident and in the administration of justice in the affected area; and
- These activities with those state and local agencies similarly engaged.

19. Military Authority

See Figure III-3.

Upon notification of Presidential approval to use military force, the Attorney General will advise the Director of the FBI, who will notify the SAC at the terrorist incident scene. The Attorney General will also notify the Secretary of Defense, who will advise the military commander. The military commander and the SAC will coordinate the



Figure III-3. Approval for Use of Military Force

transfer of operational control to the military commander. **Responsibility for the tactical phase of the operation is transferred to military authority when the SAC relinquishes command and control of the operation and it is accepted by the on-site military commander. However, the SAC may revoke the military force commitment at any time before the assault phase** if the SAC determines that military intervention is no longer required and the military commander agrees that a withdrawal can be accomplished without seriously endangering the safety of military personnel or others involved in the operation. **When the military commander determines that the operation is complete and military personnel are no longer in danger, command and control will be promptly returned to the SAC.**

For the military planner in the United States, its territories, and its possessions, **this relationship between the DOJ and Department of Defense requires the development of local memorandums of agreement or understanding between the installation, base, unit, or port and the appropriate local FBI office** to preclude confusion in the event of an incident. Because of military turnover and reorganization, these local agreements should be reviewed and tested annually.

20. Military Installation Commander's Responsibilities

a. **Domestic Incidents.** Although the FBI has primary law enforcement responsibility for terrorist incidents in the United States (including its possessions and territories), **installation commanders are responsible for maintaining law and order on military installations**. Plans should address the use of security forces to isolate, contain, and neutralize a terrorist incident within the capability of installation resources. **In the United States, installation commanders will provide the initial and immediate response to any incident occurring on military installations to isolate and contain the incident.** The FBI takes the following steps.

- The senior FBI official will establish liaison with the command center at the installation. If the FBI assumes jurisdiction, the FBI official will coordinate the use of FBI assets to assist in resolving the situation (e.g., hostage rescue team, public affairs assets).
- If the FBI assumes jurisdiction, the Attorney General will assume primary responsibility for coordinating the Federal law enforcement response.
- If the FBI declines jurisdiction, the senior military commander will take action to resolve the incident.
- Even if the FBI assumes jurisdiction, the military commander will take immediate actions as dictated by the situation to prevent loss of life or to mitigate property damage before the FBI response force arrives.
- In all cases, command of military elements remains within military channels.
- Response plans with the FBI and Service agencies should be exercised annually at the installation and base level to ensure that the plans remain appropriate.

b. **Foreign Incidents. For foreign incidents, the installation commander's responsibilities are the same as for domestic incidents — with the added requirement to notify the host nation and DOS.** Notification to the DOS is made at the geographic combatant commander level. In



Department of State embassies have the primary responsibility for dealing with terrorism against Americans abroad.

all theaters, existing plans provide guidance to the installation commander regarding notification procedures. The DOS has the primary responsibility for dealing with terrorism involving Americans abroad. **The installation's response is subject to agreements established with the host nation.** In addition, under standing rules of engagement, the inherent right of self-defense still applies in situations off-base in foreign areas. If US forces (or members thereof) are actually under attack, they retain the inherent right to respond with proportionate, necessary force until the threat is neutralized. This is providing that the host nation is unwilling or unable to respond to the threat in sufficient time or with the appropriate means.

- **The response to off-installation foreign incidents is the sole responsibility of the host nation.** US military assistance, if any, depends on the applicable status-of-forces agreement (SOFA) or MOUs and is coordinated through the US Embassy in that country. Military forces will not be provided to host-nation authorities without a directive from the Department of Defense that has been coordinated with the DOS. The degree of DOS interest and the involvement of US military forces depend on the incident site, nature of the incident, extent of foreign government involvement, and the overall threat to US security.

- AT plans will:

  •• Be implemented by geographic combatant commands, subunified commands, JTFs, and component commands, IAW responsibilities and procedures established in DODD 2000.12, "DoD Combating Terrorism Program," DODI 2000.14, "DoD Combating Terrorism Program Procedures," DODI O-2000.16, "DoD Combating Terrorism Program Standards," and DODD O-2000.12-H, "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence;"

  •• Be coordinated with and approved by the geographic combatant commander or a designated representative;

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

  •• Be coordinated by the CINC with both host-nation and DOS officials; and

  •• Be exercised annually with host-nation resources to ensure that the plan remains appropriate.

- Although the installation commander may not have security responsibility "outside the wire," he still maintains a security interest. The installation commander must include exterior terrain, avenues of approach, and host nation security processes when developing security plans for the installation, regardless of who provides exterior defense.

CHAPTER IV
ANTITERRORISM PROGRAM; INSTALLATION, BASE, SHIP, UNIT, AND PORT

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

Unknown Creole during the Haitian War for Independence, 1793

1. Overview of Program Concept

To meet the terrorist threat, **an integrated and comprehensive AT program must be developed and implemented at every echelon of command**. The program is designed to foster a protective posture in peacetime (i.e., units performing normal duties and serving in security assistance organizations, peacekeeping missions, or mobile training teams) that will carry over to a wartime environment. Antiterrorist measures are intended to identify and reduce the risk of loss or damage of potential targets and to develop procedures to detect and deter planned terrorist actions before they take place, thereby reducing the probability of a terrorist event. The measures also encompass the reactive or tactical stage of an incident, including direct contact with terrorists to end the incident with minimum loss of life and property. Antiterrorism programs should be incorporated and integrated with DODD 5160.54, "DoD Key Asset Protection Plan (KAPP)," planning, coordination, community cooperation, and synchronization, which is required for every Service, installation, base, ship, unit, and port.

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

b. **AT Program Elements.** The AT program **stresses deterrence of terrorist incidents through preventive measures** common to all combatant commands and Services. The program addresses:

- Threat analysis;
- Installation or unit criticality and vulnerability assessments;
- Creation of a threat assessment based on the threat analysis and friendly vulnerabilities;
- Information security;

- OPSEC;
- Personnel security;
- Physical security;
- Crisis management planning;
- Employment of tactical measures to contain or resolve terrorist incidents;
- Continuous training and education of personnel; and
- Public affairs planning.

c. **AT Program Concept.** The AT program concept represents an integrated, comprehensive approach within combatant commands and the Services to counter the terrorist threat to military installations, bases, ships, facilities, equipment, and personnel. Figure IV-1 illustrates this concept as it generically applies in the Services. **The concept has two phases; proactive and reactive (crisis management). The proactive phase encompasses the planning, resourcing, preventive measures, preparation, awareness education, and training that take place before a terrorist incident.** During this phase, consideration is given to research (information and intelligence gathering), development, and implementation of preventive measures; in-depth installation or facility planning (to include consideration of installation, infrastructure, and industrial targets, integration of their physical assets, force

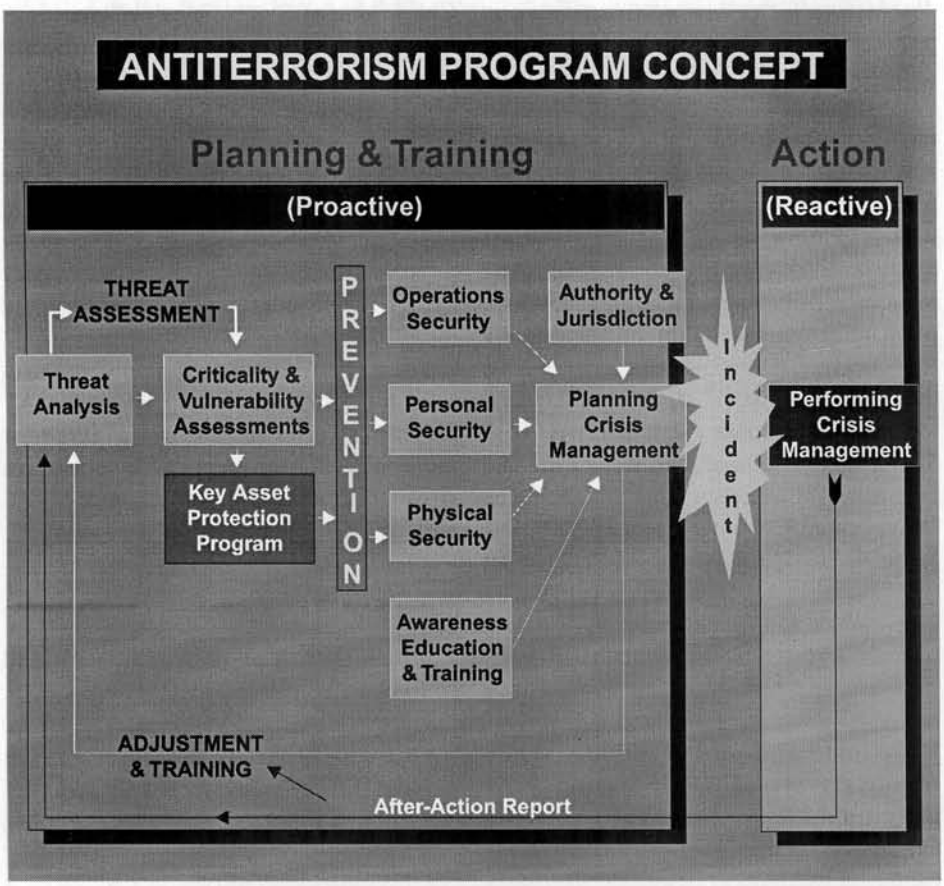


Figure IV-1. Antiterrorism Program Concept

protection funding requirements, and security forces to detect, assess, delay, and respond to a threat); and awareness education and training (specialized skills, proficiency training, and exercising plans). **The reactive phase includes the crisis management actions taken to resolve a terrorist incident.**

d. **Six-Step Concept.** The following is a brief description of the six steps in the concept. Proactive steps are discussed in more detail in Chapter V, "Intelligence, Counterintelligence, and Threat Analysis." The crisis management phase is discussed in Chapter VI, "Crisis Management Execution."

- Step 1. **Threat Assessment (Threat Analysis).** A threat analysis must be current; as data for the estimation changes, so does the risk. **Of critical importance in the threat assessment process is the analysis of criminal information and intelligence simultaneously.** Considering this information within the context of the social, economic, and political climate of an area provides a basis to determine the terrorist threat to an installation or unit. Following are the basic steps in the criminal information and intelligence process:

  •• In consonance with DODD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," collecting, evaluating, processing, and disseminating law enforcement information, intelligence, and counterintelligence from all sources, including open literature and local personnel. This is a continuous process.

  •• Formulating plans that include preparing for on-site collection and dissemination during an incident.

- Step 2. **Threat Assessment (Criticality and Vulnerability Assessments). The threat assessment brings together the threat analysis and the criticality and vulnerability assessments.** The threat assessment concerns people or items essential to the mission or function of the installation, base, ship, unit, or port. It also applies to people or facilities that, by virtue of their symbolic value to a terrorist group (as determined by the threat assessment), are probable targets. **The threat assessment is provided by the supporting counterintelligence staff element or Service counterintelligence analytical element pertaining to international terrorism.** Based on the threat assessment, the commander and staff should identify and prioritize critical personnel, facilities, and equipment, and should conduct a vulnerability assessment (VA) for each (see Appendix A, "Vulnerability Assessment"). Assessing the vulnerability of a unit, installation, base, facility, material, or personnel to the terrorist threat helps uncover and isolate security weakness. Steps can then be taken to reduce or eliminate the weakness. **Once the VA is completed, steps should be taken** (planning, training and, if necessary, design or redesign of construction projects) **to correct or reduce these vulnerabilities.** The installation commander and staff should review this VA at least annually to ensure that it remains accurate in view of the changing threat, installation makeup, and unit missions.

- Step 3. **Prevention.** The prevention portion of the concept consists of **four separate but related elements** that together provide a synergistic effect in reducing the vulnerability of an installation, base, facility, unit, or

personnel to terrorist attack. **The elements are OPSEC, personal security (including travel), physical security, and awareness education and training.**

•• **Operations Security.** A threat assessment may reveal security weaknesses in day-to-day operations. The security of communications systems, information activities, and personnel must be examined and weakness corrected to include countersurveillance techniques when necessary. Information gleaned from communications can provide terrorists with detailed knowledge about potential targets. Communications security is an integral part of OPSEC. Terrorists are not hampered by regulations and fully exploit opportunities presented to them. **The objectives of OPSEC as they pertain to AT are** shown in Figure IV-2.

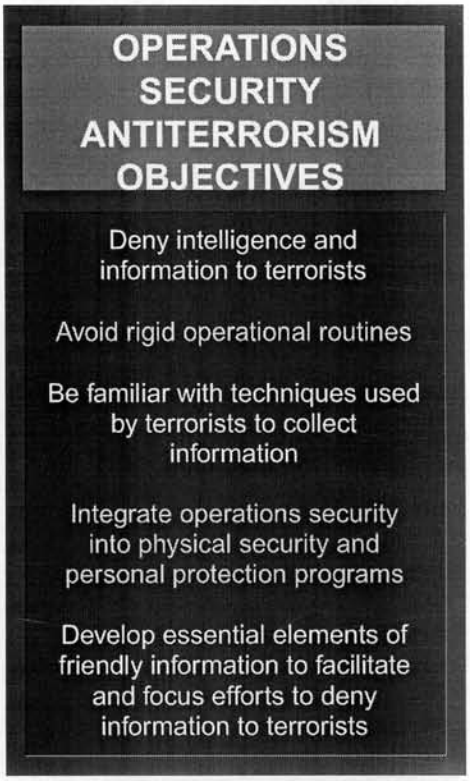


Figure IV-2. Operations Security Antiterrorism Objectives

•• **Personal Security.** All military **personnel** and family members, as well as civilians connected with the military or US Government (including contract personnel) **are potential victims of terrorist attacks and should take the basic security precautions outlined in Appendix B**, "Personal Protective Measures Against Terrorism." A VA may identify specific personnel who, by virtue of their rank, position, travel itinerary, or symbolic value, may become particularly attractive or accessible targets. Prevention of such attacks depends on the planning and the use of the personal protection measures outlined in Appendix C, "Very Important Person and Senior Officer Security Measures." **The most important measure is in educating persons who are likely targets in recognition of threat and taking appropriate actions to reduce their risk.** Personal protection, education, and training must emphasize how to deny the opportunity for an attack or to elevate the risk to the attacker. The objective of personal protection is to use personal protection measures tailored to the level of the threat.

•• **Physical Security.** Physical security measures for an installation, base, ship, unit, or port reduce the probability for terrorist attack by making an attack more difficult and increasing the risk to the terrorist. **The installation, base, ship, unit, or port should be assessed in terms of defensive capability.** The integrated use of intrusion detection systems, barriers, structural hardening, access control, and response forces are critical to the detection of a threat, assessment of the threat, and delaying the threat until arrival of the security forces. These measures are designed to prevent

unauthorized access to installations, bases, facilities, equipment, materiel, and information as well as to safeguard against espionage, terrorism, sabotage, vandalism, and theft. The more an area's physical security is enhanced, the greater the delay to the terrorist trying to reach the objective and the more time security forces have to detect, deter and/or intercept the terrorist. Measures that enhance physical security include intrusion detection systems; proper use of lighting and fences; restricting access to an installation, base, ship, unit, port, or facility; secure sensitive storage locations; structural hardening; and well-trained security personnel. Appendix D, "Building Security Procedures," Appendix E, "Lock Security," and Appendix F, "Telephone Call Procedures," provide detailed suggestions for physical security measures. The objective of physical security as it pertains to antiterrorism is to identify physical vulnerabilities of installations, personnel, and materiel to terrorist attacks and to take appropriate actions to reduce or eliminate those vulnerabilities.

- **Awareness Education and Training.** (See DODI O-2000.16, "DoD Combating Terrorism Program Standards," for specific guidance on AT training standards.) **The key to an effective AT program is to develop an awareness that is both sustained and reinforced as the Service member progresses** from initial entry to termination of a military career. Appendix B, "Personal Protective Measures Against Terrorism," lists personal protective measures that should be widely disseminated periodically throughout the Services. To complement this, the member must be trained in the techniques of personal protection and security commensurate with the threat in his or her locale. (1) **Functional Training. Personnel whose duties require special security skills must also be trained.** For example, the following personnel cannot perform their mission without specialized training: members of the reaction force; hostage negotiators; members of the protective services (especially those assigned to the close-in protective service detail and team leaders); drivers for high-risk personnel; installation, base, or unit AT planners;



Physical security forces are designed to intercept terrorists before they are able to reach their objective.

and personnel responsible for the terrorist analysis input to the installation, base, or unit threat analysis. In addition, appropriate members of the installation planning team should be trained in installation and facility physical security planning; such training is offered by the US Army Corps of Engineers and the US Army Military Police School (USAMPS). (2) **High-Risk Positions.** These are **key and essential positions that, because of grade, assignment, travel itinerary, or symbolic value, may make them especially attractive or assessable terrorist targets.** Reporting to higher headquarters is an important element in any threat or terrorist situation. High-risk positions are identified and so designated by the combatant commander based on the following considerations: (a) Location; and (b) Security situation with respect to work area, housing, areas of travel, assessment of criminal threat, evaluation of host-nation security, position sensitivity and visibility, and anticipated political environment. Combatant commanders annually aggregate the list of high-risk positions, forwarding them through the appropriate Service personnel channels to enable each Service to input training requirements by 30 June. All personnel and adult family members en route to high-risk positions should attend the Individual Terrorism Awareness Course conducted by US Army John F. Kennedy Special Warfare Center, Fort Bragg, North Carolina. During this 1-week course, personnel will receive instruction in defensive driving techniques and survival shooting as well as individual protective measures and hostage survival. These individuals should also attend the appropriate Regional Orientation Course (Middle East, Asia-Pacific, Latin America, or Africa) offered at the US Air Force Special Operations School, Hurlburt Field, Florida. Before assuming duties, the Service member who will be required to frequently operate a vehicle should attend the Evasive Driving for Senior Officers Course conducted by USAMPS, Fort McClellan, Alabama, or (for Air Force members) the Senior Officer Security Seminar, Air Force Special Investigations Academy, Bolling AFB, Washington, DC. (3) **Protective Training.** Personnel en route to potential high threat areas should attend one of the following courses: (a) The Dynamics of International Terrorism Course conducted at the US Air Force Special Operations School at Hurlburt Field, Florida. During this 1-week course, personnel will receive lectures on threats by region (Europe, Middle East, Latin America, Asia-Pacific, and Africa), the history and psychology of terrorism, personnel AT measures (vehicle, personal, airline, and physical security), and hostage survival. (b) A Regional Orientation Course (Middle East, Latin America, Africa, Asia-Pacific) at the US Air Force Special Operations School at Hurlburt Field, Florida. These courses provide instruction in cultural, political-military, and individual security factors associated within the specific region. (c) Training may also be given by installation security personnel who have been trained at the Antiterrorism Instructor Qualification Course at Fort Bragg, North Carolina, or the Force Protection Unit Advisors Course at Fort McClellan, Alabama.

- Step 4. **Authority and Jurisdiction.** Because an understanding of who has authority and responsibility is an essential part of any plan, this publication includes authority and jurisdiction as a program element. Chapter III, "Legal Considerations," outlines the responsibilities of the

Department of Defense, DOJ, DOT, USCG, and DOS in terrorist incidents.

- Step 5. **Planning Crisis Management. The establishment of a mechanism to respond to a terrorist incident is an essential element of the AT program.** Normally, the installation, base, or unit commander identifies an office or section or designates personnel from various sections who act as the principal planning agency for special threats, and who comprise the operations center during an actual crisis. This office creates a crisis management plan to meet the threat (see Appendix G, "Crisis Management Plan Format"). Crisis management planning must address the activation and responsibilities of local resources and provide mechanisms to obtain the support of resources not under local control (e.g., public affairs officer [PAO], legal, medical, and aviation resources, and EOD). A detailed checklist is provided in Appendix H, "Crisis Management Plan Checklist."

- Step 6. **Performing Crisis Management Operations.** As the threat increases, a series of graduated DOD THREATCONs dictate prescribed actions (DODD 2000.12, "DoD Combating Terrorism Program").

2. Implementing the Concept

a. **Installation Commanders.** Commanders directly responsible for operating bases, ships, ports, stations, facilities, and centers in the United States and foreign areas are termed installation commanders. **These individuals are responsible for the overall security and protection of the installation and personnel by establishing AT programs.** This responsibility includes the security of personnel, equipment, materiel, and facilities. To implement the AT program, the installation commander directs functions to be performed as shown in Figure IV-3.

b. **Preventive Planning. Installation commanders with tenant command representation form a preventive planning organization.** The planning organization is normally composed of those individuals who compose the operations center during crisis management, as well as additional staff representation from special offices such as the budget or civilian personnel offices. The planning organization will establish a threat committee to assess current threat information. A threat assessment should be conducted at least annually. These individuals are responsible for the security and protection of the installation, and an effective AT program is a critical element of this effort. The preventive planning organization should include staff from operations, intelligence, counterintelligence, law enforcement and/or security forces, engineers, legal, public affairs, and an NBC representative to the preventive and crisis management committee. This organization should consider the installation from an AT perspective to assess the threat, integrate the installation's physical features with its security force capabilities, develop plans to compensate for weaknesses, and recommend enhancements (including education and awareness programs) that reduce installation vulnerabilities and improve detection and assessment capabilities.

c. **Crisis Management Planning.** Installation commanders designate a specific office or selected staff members (often the military law enforcement authority or operations staff agency) to **form an organization to plan and coordinate the command's AT efforts during training and to serve as the operations center** during training exercises and actual crises. Because the members of this organization are also members of the preventive planning organization, the organization knows the key

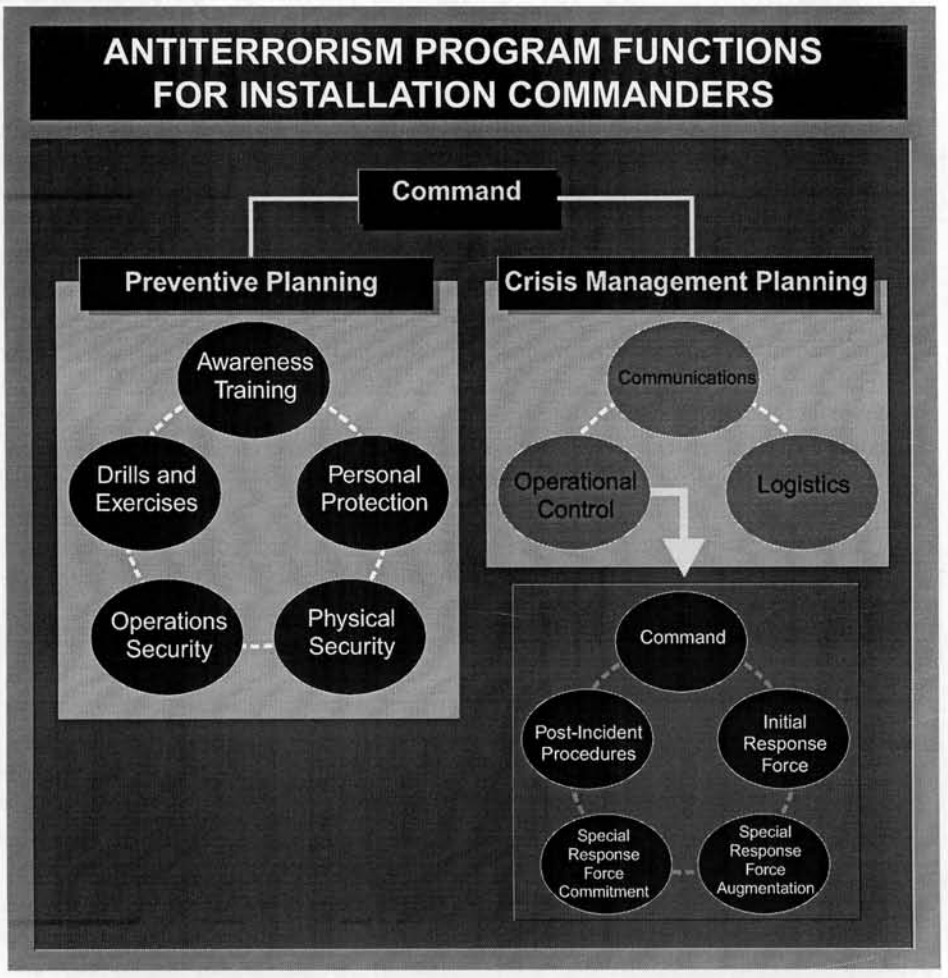


Figure IV-3. Antiterrorism Program Functions for Installation Commanders

infrastructures and assets critical to the installation's operation. To be successful, members must be predesignated, train together, and be prepared to perform individual and collective crisis management missions under the control of the installation commander or the designated representative. Tenant commanders may also serve or have staff representation in this organization. The most common participants in the crisis management organization are listed in Figure IV-4.

- **Operational Control and Coordination Center (Operations Center). A predesignated location for the operations center must be readily available.** The operations center functions by predetermined standing operating procedures (SOPs). As dictated by these SOPs, predetermined and adequate communications systems must be made available at the location. Operational SOPs can be stressed and validated during normally scheduled AT evaluation exercises.

- **Operational Response Forces.** The installation commander **predesignates and trains personnel to serve as a response force at the incident location.** This force is trained and equipped to

CRISIS MANAGEMENT PARTICIPANTS

- -Personnel
- -Intelligence and/or Security
- -Operations
- -Counterintelligence
- -Logistics
- -Civil Affairs
- -Special Staff Sections:
  - --Military Law Enforcement Authorities
  - --Legal
  - --Public Affairs
  - --Transportation
  - --Aviation
  - --Communications
  - --Engineers and/or Utilities
  - --Medical Activity and/or Red Cross
  - --Chaplain
  - --Psychologist
  - --Explosive Ordnance Disposal
- -Major Tenant Commands
- -Local Investigative Field Office (e.g., Criminal Investigation Division, Naval Criminal Investigative Service Command
- -Civilian Authorities and/or Representatives
- -Federal, State, Local, or Host-Nation Police
- -Host-Nation Military and Intelligence Activities at Overseas Locations

Figure IV-4. Crisis Management Participants

isolate and contain the incident until representatives from the FBI or host-nation forces arrive at the scene and, if necessary, resolve the incident. Force protection funds are available within the Department of Defense for installations to train and equip these response forces. Respective Service resource management offices will provide points of contact for coordinating access to these funds. Figure IV-5 illustrates normal functions performed by the operational response force.

d. **Tenant and Transient Commanders.** Commanders who are not under the control of the installation commander but are assigned or attached to the installation are tenant commanders. If all forces are from one Service, then Service doctrine for base defense will apply. If the installation has tenants from more than one Service, the provisions of Joint Pub 3-10, "Doctrine for Joint Rear Area Operations," Chapter II, Paragraph 3b apply. Tenant commanders are still responsible for their command's physical security and for terrorism planning not provided by the installation or base commander. If the forces concerned meet the definition of transient forces, the provisions of Joint Pub 0-2, "Unified Action Armed Forces (UNAAF)," Chapter IV, Paragraph 1b apply.

3. Threat Conditions

The mechanism by which the AT program operationally increases or decreases protective measures is **the DOD THREATCON System** (Appendix J, "THREATCON System"). As a DOD-approved system, the terms, definitions, and prescribed security measures are intended to facilitate inter-Service coordination, reporting, and support of US military AT activities. Selection of the appropriate response to terrorist threats remains the responsibility of the commander having jurisdiction or control over threatened facilities or personnel.

4. Combatant Commander's Responsibility

The geographic combatant commander designates a staff office, usually in the Operations Division, law enforcement, or

ON-SITE OPERATIONAL RESPONSE STRUCTURE		
SECURITY	REACTION/ MANAGEMENT	SUPPORT
Military Police/Security Forces (on duty/on call)	Control Staff	Logistics Personnel Intelligence Counterintelligence
Police Reaction/Assault Force	Negotiations Personnel	Fire Department
Guard Forces	Liaison Personnel	Explosive Ordnance Disposal
Auxiliary Security Forces	Public Affairs	Medical Personnel
	Staff Judge Advocate	Communications Personnel

Figure IV-5. On-Site Operational Response Structure

security section, to supervise, inspect, test, and report on the base AT programs within the theater. This staff section also coordinates with host-nation authorities and US embassies. Simultaneously, the Intelligence Directorate of a joint staff (J-2), under the combatant commander's authority, disseminates intelligence on terrorist activities to the subordinate commands to ensure that the AT measures are appropriate to the threat. The manner in which the geographic combatant commander places importance on these staff functions usually has a direct affect on the AT readiness of subordinate commands.

CHAPTER V
INTELLIGENCE, COUNTERINTELLIGENCE, AND THREAT ANALYSIS

". . .we must recognize the appearance of a new and particularly dangerous form of attack. I refer to subversive insurgency, supported from the outside against legitimate free governments."

General Maxwell Taylor

SECTION A. INTELLIGENCE AND COUNTERINTELLIGENCE

1. Intelligence and Counterintelligence Support

Intelligence and counterintelligence are **the first line of defense in an AT program**. A well-planned, systematic, all-source intelligence and counterintelligence program is essential. The role of intelligence and counterintelligence is to identify the threat, provide advance warning, and disseminate critical intelligence in a usable form for the commander. Additionally, counterintelligence provides warning of potential terrorist attacks and provides information for CT operations. This chapter provides the reader with the elements of the intelligence cycle that have particular importance in a viable AT program. Effective intelligence and counterintelligence support requires effort, planning and direction, collection and analysis, production, investigations, and dissemination. The entire process is important in providing decision makers with information and timely warnings upon which to recommend AT actions.

2. Sources

The **primary sources** of intelligence and counterintelligence for the AT program are **open-source information, criminal records, government intelligence, and local information**. (See Figure V-1.)



Figure V-1. Sources of Intelligence and Counterintelligence

a. **Open-Source Information.** This information is **publicly available and can be collected, retained, and stored without**

special authorization. The news media are excellent open sources of information on terrorism. The news media report many major terrorist incidents and often include in-depth reports on individuals, groups, or various government counterstrategies. Government sources include congressional hearings; publications by DIA, FBI, the Central Intelligence Agency (CIA), and DOS; and the national criminal justice reference services. Additionally, there are private data services that offer timely information on terrorist activities worldwide. Terrorist groups and their affiliates may also have manuals, pamphlets, and newsletters that reveal their objectives, tactics, and possible targets. Open sources are not a substitute for classified capabilities, but they can provide a valuable foundation and context for rapid orientation of the analyst and the consumer and for the establishment of collection requirements which take full advantage of the unique access provided by classified sources.

b. **Criminal Records. Both military and civil law enforcement agencies collect criminal records.** Because terrorist acts are criminal acts, criminal records are a major source for terrorist intelligence. Commanders must work through established law enforcement liaison channels because the collection, retention, and dissemination of criminal records are regulated. Local military criminal investigative offices of the US Army Criminal Investigations Command (USACIDC), Naval Criminal Investigative Service (NCIS), Air Force Office of Special Investigations (AFOSI), and Headquarters, US Marine Corps, Criminal Investigations Division, maintain current information that will assist in determining the local terrorist threat.

c. **Government Intelligence. The Community Counterterrorism Board is responsible for coordinating the national intelligence agencies concerned with combatting international terrorism.** These agencies include the CIA (lead agency), DIA, National Security Agency, DOS, DOJ, FBI, the Department of Energy, the DOT, USCG, FAA, Federal Communications Commission, and the Department of Defense. Service intelligence and counterintelligence production organizations that compile comprehensive intelligence and counterintelligence from these agencies for distribution on a need-to-know basis throughout the Services include: the Army Counterintelligence Center; the Navy Antiterrorism Alert Center; Headquarters, US Marine Corps, Counterintelligence; and Headquarters, AFOSI. In combatant commands, the J-2 is responsible for the integration of intelligence policy issues across the command staff. The counterintelligence support officer (CISO) provides counterintelligence interface between the combatant command, the component commands, and the Joint Staff.

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

3. Responsibilities of US Government Lead Agencies

a. **General. The FBI is responsible for collecting and processing domestic terrorist information. Overseas, terrorist intelligence is principally a CIA responsibility**, but the DOS, DIA, and host nation are also active players. Military intelligence activities are conducted in accordance with Presidential Executive

SHINING PATH

Shining Path (in Spanish, *Sendero Luminoso*) sprung up in the isolated Andean department of Ayacucho, one of the poorest regions of Peru. Its roots were embedded in the Sino-Soviet split of 1963, when a small circle of university lecturers led by Abimael Guzman formed a core group within the break-away, pro-China faction of the Peruvian Communist Party.

The faction's ideology is an idiosyncratic mixture of the theories of Marx, Lenin and Mao, mainly Mao, knotted together by Guzman in accordance with his analysis of the history and social realities of Peru. In claiming to be the "fourth sword" of communism, Guzman conceives himself as carrying on where Marx, Lenin and Mao left off, partly intellectually, but mainly in being at the vanguard of international communist revolution, which he regards as a scientific-historical inevitability temporarily betrayed by revisionists in the hands of reactionary imperialists. Guzman's achievement rests in molding a cohesive body of thought sufficiently relevant to Peru for it to have inflamed university lecturers, industrial workers and illiterate peasants alike.

Shining Path divides combat into four forms: "armed" propaganda such as slogan painting, enforced radio broadcasts and street rallies; sabotage aimed at suffocating the state economy; "selective" killings, targeting people in key positions opposed to them, whether state authorities, political leaders, priests, businessmen or, in their context of being "government collaborators," foreign and local aid workers; and guerrilla warfare to take on the security forces and army-backed peasant militia.

SOURCE: Simon Strong
Shining Path: A Case Study in Ideological Terrorism
Research Institute for the Study of Conflict and Terrorism, April 1993

orders, Federal law, SOFAs, MOUs, and applicable Service regulations.

b. **Responsibilities of Intelligence Activities.**

- **The geographic combatant commander,** through the commander's J-2 Joint Intelligence Center and the CISO and in consultation with DIA, CIA, embassy staff, country team, and applicable host-nation authorities, **obtains intelligence and counterintelligence specific to the operational area** and issues intelligence and counterintelligence reports, advisories, and assessments to the units within the combatant command's control or operating within the combatant command's AOR. This network is the backbone for communicating intelligence and counterintelligence information, advisories, and warning of terrorist threats throughout the region.

- DODD 2000.12, "DoD Combating Terrorism Program," tasked **the Secretaries of the Military Departments to ensure that a capability exists to collect, receive, evaluate from a Service perspective, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack.** To accomplish this task, each Secretary appoints a military intelligence or counterintelligence agency (US Army Intelligence and Security Command,

NCIS, AFOSI) to conduct intelligence and counterintelligence activities directed against terrorists and to detect, neutralize, or deter terrorist acts. To accomplish this mission, the Military Department intelligence agency establishes, as needed, counterintelligence offices on an area basis to collect and disseminate information to combatant commanders. Each Military Department intelligence agency is responsible for the following:

•• Provides overall direction and coordination of the Service counterintelligence effort.

•• Operates 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.

•• Provides Service commanders with information on terrorist threats concerning their personnel, facilities, and operations.

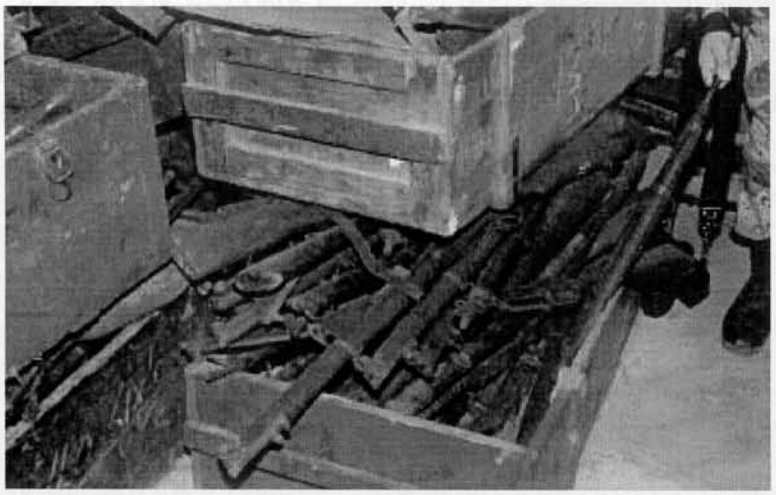
•• With the FBI or host-nation authorities, investigates terrorist incidents for intelligence, counterintelligence, and force protection aspects.

•• Provides terrorist threat information in threat briefings.

•• Conducts liaison with representatives from Federal, state, and local agencies as well as host-nation agencies to exchange information on terrorists.

•• Provides international terrorism summaries and other threat information to supported commanders. On request, provides current intelligence and counterintelligence data on terrorist groups and disseminates time-sensitive and specific threat warnings to appropriate commands.

- **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



Success in thwarting terrorist activities requires a coordinated intelligence effort from several US government agencies.

security forces and civilian law enforcement agencies.

- **Intelligence staff elements of commanders at all echelons** will:

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

  •• Initiate and maintain liaison with the security forces or provost marshal's office, local military criminal investigative offices, local counterintelligence offices, security offices, host-nation agencies, and (as required or allowed by law or policy) other organizations, elements, and individuals.

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

- **Law enforcement staff elements** will be responsible for the following:

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

  •• Initiate and maintain liaison with local counterintelligence offices and military criminal investigative offices.

  •• Maintain liaison with Federal, host-nation, and local law enforcement agencies or other civil and military AT agencies as appropriate.

- **Installation, base, ship, unit, and port security officers** will be responsible for the following:

  •• Report all actual or suspected terrorist incidents or activities to their immediate commander, supporting military law enforcement office, other supported activities, local counterintelligence office, and local military criminal investigation office.

  •• Conduct regular liaison visits with the supporting military law enforcement office, counterintelligence office, and local criminal investigation office.

  •• Coordinate with the supporting military law enforcement office and counterintelligence offices on their preparation and continual updating of the threat assessments.

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

4. Information Requirements

To focus the threat analysis, **intelligence and counterintelligence officers develop information requirements (IRs) for identifying potential terrorist targets** based on existing knowledge of an organization. Terrorist group IRs are shown in Figure V-2.

SECTION B. THREAT ASSESSMENT

5. Preparation of Threat Analysis

Terrorist threat analysis **is a continual process of compiling and examining all available information in order to identify terrorist targeting of US interests.** A vulnerability analysis is a continual process of compiling and examining information on the security posture of a facility. The threat analysis is then paired with the facility's

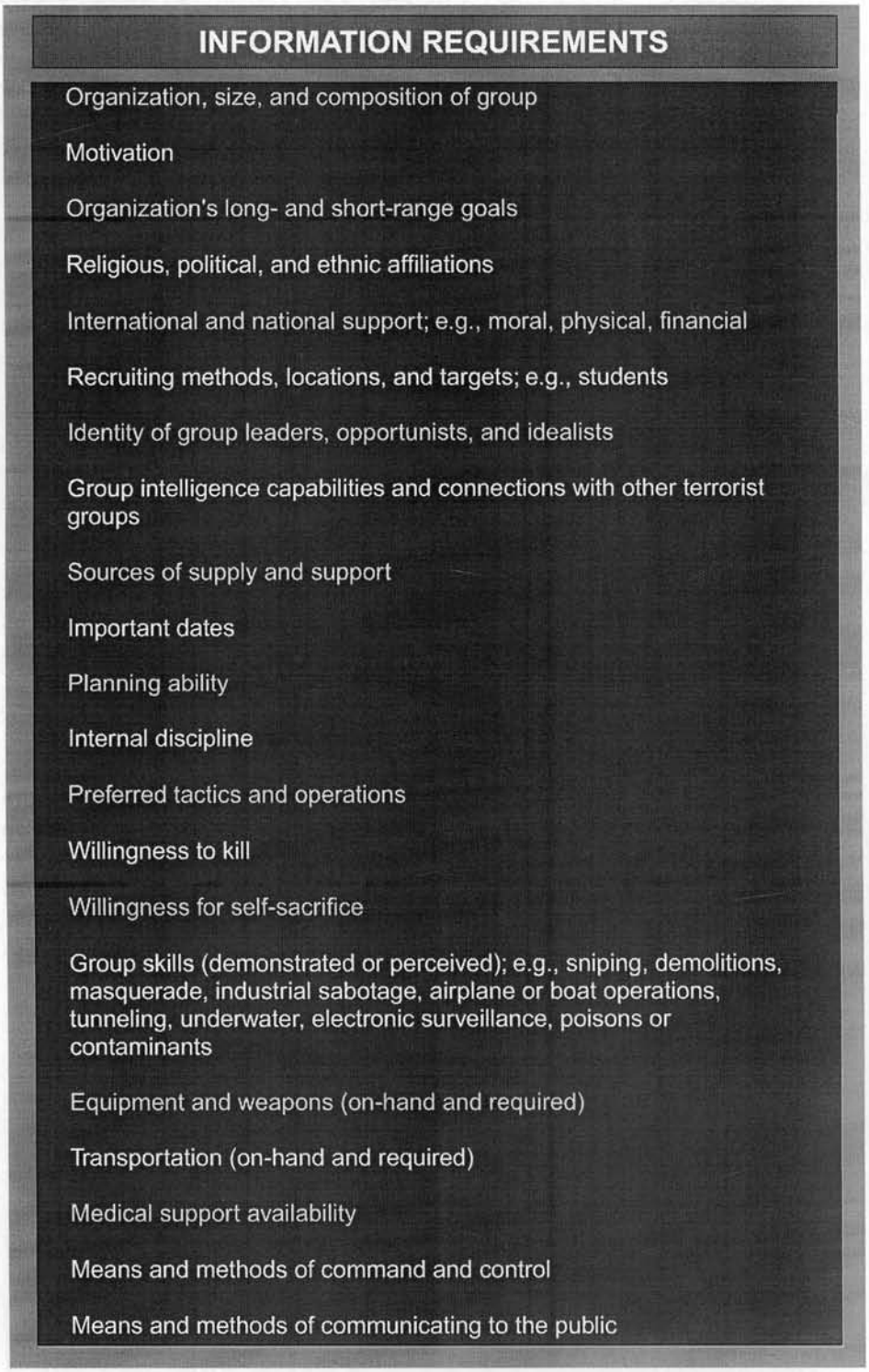


Figure V-2. Information Requirements

vulnerability analysis to create the threat and vulnerability assessment. **Threat analysis is an essential step in identifying probability of terrorist attack.** To enhance this capability to collect and analyze information from many sources, DIA maintains a terrorism data base on the Migration Defense Intelligence Threat Data System and the combatant command's J-2; the CISO, in consultation with DIA, focuses this data base information and regional information toward the intelligence and counterintelligence needs specific to the security of the command. Country threat assessments and information about terrorist organizations, biographies, and incidents in the data base are disseminated to the commands and Services. Commands at all echelons then augment or refine the DIA's analyses to focus on their area of interest. This process is operative across the range of military operations, promotes coordination between all levels of the intelligence, counterintelligence, and law enforcement communities, broadens acquisition channels, and enhances timely distribution of information to the supported commander.

a. **Several factors complicate intelligence and counterintelligence collection and operations.** The small size of terrorist groups, coupled with their mobility and cellular organization, make it difficult to identify the members. Unlike other criminals, terrorist cadres often receive training in counterintelligence and security measures from foreign intelligence agencies or other terrorists. Additionally, the traditional orientation of police organizations is toward individual criminals, while military intelligence organizations focus on conventional forces. Terrorist activity, therefore, requires some degree of reorientation for police and military intelligence and counterintelligence collection and operations.

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

c. **Commanders must carefully exercise judgment in estimating both the existing terrorist threat and the need for changes in antiterrorism measures.** Commanders should consider the following key questions:

- What has changed (mission, political climate, installation and unit personnel or equipment, terrorist capabilities)?
- What affect will the changes have on the security posture?

Extraordinary security measures, unless part of a deliberate deception during critical or high-threat situations, **draw attention and detract from mission accomplishment.** Sound physical security, personnel who are aware, an accurate threat assessment, and well-rehearsed response plans reduce the probability of a successful terrorist venture. The aim is to make an attack too difficult or the level of risk unacceptable to the terrorist. However, the ability of the terrorists to react quickly and adapt swiftly in modifying their own tactics, techniques, and procedures cannot be overlooked.

d. A threat analysis should be written to the factors below:

- **Factor 1, Existence:** A terrorist group is present, assessed to be present, or able to gain access to a given locale.
- **Factor 2, Capability:** The acquired, assessed, or demonstrated level of capability to conduct terrorist attacks.

- **Factor 3, Intentions:** Recent demonstrated anti-US terrorist activity, or stated and/or assessed intent to conduct such activity.

- **Factor 4, History:** Demonstrated terrorist activity over time.

- **Factor 5, Targeting:** Current credible information on activity indicative of preparations for specific terrorist operations and/or specific intelligence which shows that an attack is imminent.

- **Factor 6, Security Environment:** The internal political and security considerations that impact on the capability of terrorist elements to carry out their operations.

e. To determine the level of threat, see Figure V-3.

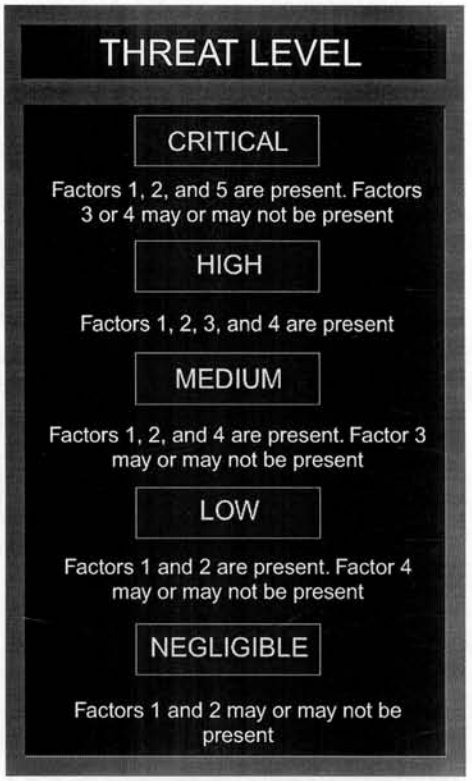


Figure V-3. Threat Level

6. Preparation of Criticality and Vulnerability Assessments

Having obtained a threat analysis, the commander and staff proceed to complete the threat assessment by conducting **the criticality and vulnerability assessments. This process considers the following:**

a. **Mission.** A review and analysis of the mission of the installation, base, ship, unit, or port in relation to the terrorist threat. The review should assess the cost of AT measures in terms of lost or reduced mission effectiveness. Often the best operational method and routine may be the worst to counter potential terrorist activities. It should then assess the level of acceptable risk to facilities and personnel given the estimated erosion of mission effectiveness. This review and analysis is performed routinely and particularly for deployment.

b. **Installation, Base, Ship, Unit, or Port Assessment.** This step combines the results of the following considerations to create the installation, base, ship, unit, or port assessment. The assessment provides the staff with the overall vulnerability to terrorist attack. The staff then develops the crisis management plan (see Appendix G, "Crisis Management Plan Format") from this assessment. The crisis management plan addresses all terrorist threat levels regardless of the present level. THREATCONs (see Appendix J, "THREATCON System") are then applied in accordance with the local threat. The considerations are as follows:

- **Vulnerability.** The VA is a self-assessment tool. The installation, base, ship, unit, or port uses the VA to evaluate its vulnerability to terrorist attack. The more vulnerable an installation, base, ship, unit, or port is, the more attractive it becomes to terrorist attack. Appendix A, "Vulnerability Assessment,"

provides a guide to developing an assessment capability.

- **Criticality.** The criticality assessment identifies key assets and infrastructures located on and adjacent to the installation, base, ship, unit, or port, such as the existence of symbolic targets that traditionally appeal to a specific terrorist group (e.g., headquarters, buildings and monuments). It addresses the impact of temporary or permanent loss of key assets or infrastructures to the ability of the installation, base, ship, unit, or port to perform its mission. The staff determines and prioritizes critical assets. The commander approves the prioritized list. The assessment:

  •• Selects key assets;

  •• Determines whether critical functions can be duplicated under various attack scenarios;

  •• Determines time required to duplicate key assets or infrastructure efforts if temporarily or permanently lost;

  •• Determines vulnerability of key assets or infrastructures to bombs, vehicle crashes, armed assault, and sabotage; and

  •• Determines priority of response to key assets and infrastructures in the event of fire, multiple bombings, or other terrorist acts.

- **Damage.** The damage assessment determines the ability of the installation, base, ship, unit, or port to plan for and respond to a terrorist attack against key assets and infrastructures.

- **Recovery Procedures.** The recovery procedures assessment determines the capability to recover from the temporary or permanent loss of key assets and infrastructures. Based on this assessment, the staff establishes recovery procedures to ensure the continued ability to perform the mission.

7. 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, or port to respond. Drills and exercises test suspected vulnerabilities and AT measures. These exercises and drills also train the staff as well as reaction force leadership and help maintain a valid threat assessment by identifying and adjusting to changing threat capabilities as well as installation, base, ship, unit, or port vulnerabilities.

Intentionally Blank

CHAPTER VI
CRISIS MANAGEMENT EXECUTION

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

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

1. General

Chapter IV, "Antiterrorism Program; Installation, Base, Ship, Unit, and Port," structured the framework for an integrated AT program. This chapter provides commanders with a specific view of the program as an incident occurs. When the program is challenged, **crisis management execution requires special considerations, which are shown in Figure VI-1.**

2. Initial Response

Either on-duty military law enforcement patrols or guard personnel usually provide initial response to a terrorist attack. The initial response force is under the control of the on-scene senior officer or noncommissioned officer or senior enlisted person who has assumed responsibility. Once the initial response force has responded to the incident and determined the circumstances, the installation commander activates required forces and begins notification procedures to military and civilian authorities.

a. **Initial Response Force. The initial response force immediately identifies and reports the nature of the situation, isolates the incident, and contains the situation until relieved by the reaction force commander.** Initial response force actions are critical. Each shift of the daily security force must have trained personnel who are aware of the threat and are capable of reacting promptly to any new development. For example, if the attack is a bombing, ambush, assassination, or firebombing, the terrorists may escape before additional forces arrive. In these cases, the initial response force provides medical aid, seals off the crime scene, and secures other potential targets in case the initial attack was a diversionary tactic. If the event is a hostage or barricade situation, the initial response force seals off and isolates the incident scene to ensure that 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. For foreign incidents, the initial response force must be prepared to interface with host-nation police or military forces that may also be responding to the incident.

b. **Installation, Base, Ship, Unit, or Port Commander.** The commander, depending upon established SOPs, **activates the command center, notifies specialized response forces, and immediately reports the incident** to the appropriate superior military command operations centers, military investigative agency, FBI, civilian authorities and, if a foreign incident, to host-nation authorities as required.

c. **The Operations Center.** The operations center **serves as the command post at a predetermined location.** Communications are immediately established with the initial response force containing the situation, the specially trained operational response force preparing to take over or augment the initial response force, and other critical participants as predesignated in the operational center's SOPs. There are usually three standard secure communications circuits: command net (administrative

CRISIS MANAGEMENT EXECUTION CONSIDERATIONS

- Awareness of the possibility of multiple incidents or diversionary tactics
- Activation of required resources by combatant commander and base under attack
- Notifications to the combatant command, appropriate military investigative agency, FBI, and host-nation officials
- Exercise of the public affairs officer's role with news media
- Negotiation, if the situation requires it
- Implementation of tactical measures to contain or defeat the threat
- Preparation of after-action measures to protect the evidence, handle captured personnel, identify and process hostages, document actions for use in prosecution, and identify needed changes to the existing antiterrorism plan

Figure VI-1. Crisis Management Execution Considerations

matters, support, routine traffic), tactical net (operations), and intelligence net. The tactical net may be divided in order to accommodate the myriad of security activities that transpire on a large military installation during an emergency situation. Ideally, static posts should be on one tactical net, the mobile patrols on another, and other patrols unique to the installation on yet another frequency. If necessary, a dedicated net for negotiations may be necessary if a landline cannot be established with the terrorists.

d. **Confirmation.** Because jurisdiction depends on whether the crime is a terrorist incident, **the response force must identify the type of incident as quickly as possible**. If the FBI or host nation assumes control, then the response force must be prepared to coordinate the operational handover and assist as needed. For example, the initial or specialized response forces may be required to provide outer perimeter security while the FBI or host-nation forces take over responsibility for the inner perimeter security and the handling of the situation. At the same time, the operational coordination and control center, as well as the response forces, must be prepared to manage the entire event if the FBI or host nation either does not assume control or relinquishes control. **The key here is for the installation, base, ship, unit, or port forces to always prepare for the worst possible contingency.** This level of readiness requires considerable sustainment training.

3. Response

The response to a terrorist incident varies depending on the nature and location of the incident. Recognizing that many incidents do not develop beyond the first phase, **there are generally three distinct phases** (shown in Figure VI-2) through which an incident may evolve.

a. **Phase I is the commitment of locally available resources.** This includes available

TERRORIST INCIDENT PHASES

PHASE ONE

The commitment of locally available resources - military law enforcement personnel, security force patrol or guards, and available backup units

PHASE TWO

The augmentation of the initial response force by additional law enforcement and security personnel and/or a specially trained response force

PHASE THREE

The commitment of the specialized Federal Bureau of Investigation, Department of Defense, or host-nation counterterrorist force

Figure VI-2. Terrorist Incident Phases

military law enforcement personnel, security force patrols or guards, and available backup units. Ideally, all law enforcement or security personnel are familiar with local SOPs for terrorist incidents and have practiced these procedures as part of their unit training program. They must be prepared to secure, contain, and gather information at the scene until the beginning of Phase II. Because terrorist incidents often include diversionary tactics, response forces must be alert to this fact while securing and containing the incident scene. The evacuation of threatened areas is a priority function.

b. **Phase II is the augmentation of the initial response force by additional law enforcement and security personnel and/or a specially trained response force — special reaction team, emergency services team, FBI regional special weapons and tactics units or the hostage rescue teams, or host-nation tactical units.** This phase begins when the operational center is activated. During this phase, either the FBI or the host nation may assume jurisdiction over the incident. If that occurs, military forces must be ready to support the operation. The installation, base, ship, unit, or port specially trained reaction force must be ready for employment in this phase of the operation. In any country in which a terrorist incident against an American facility or unit occurs, the DOS and the US Embassy will play the key role in coordinating the US Government and host country response to such an incident.



Joint forces must be prepared to play an active security role throughout all three terrorist incident phases.

c. **Phase III is the commitment of the specialized FBI, DOD, or host-nation counterterrorist force.** This is the phase in which steps are taken to terminate the incident. Incident termination may be the result of successful negotiations, assault, or other actions including terrorist surrender. Because identifying the terrorists, as opposed to the hostages, may be difficult, capturing forces must handle and secure all initial captives as possible terrorists.

d. **Response Sequence.** A typical response sequence to a terrorist incident is shown in Figure VI-3.

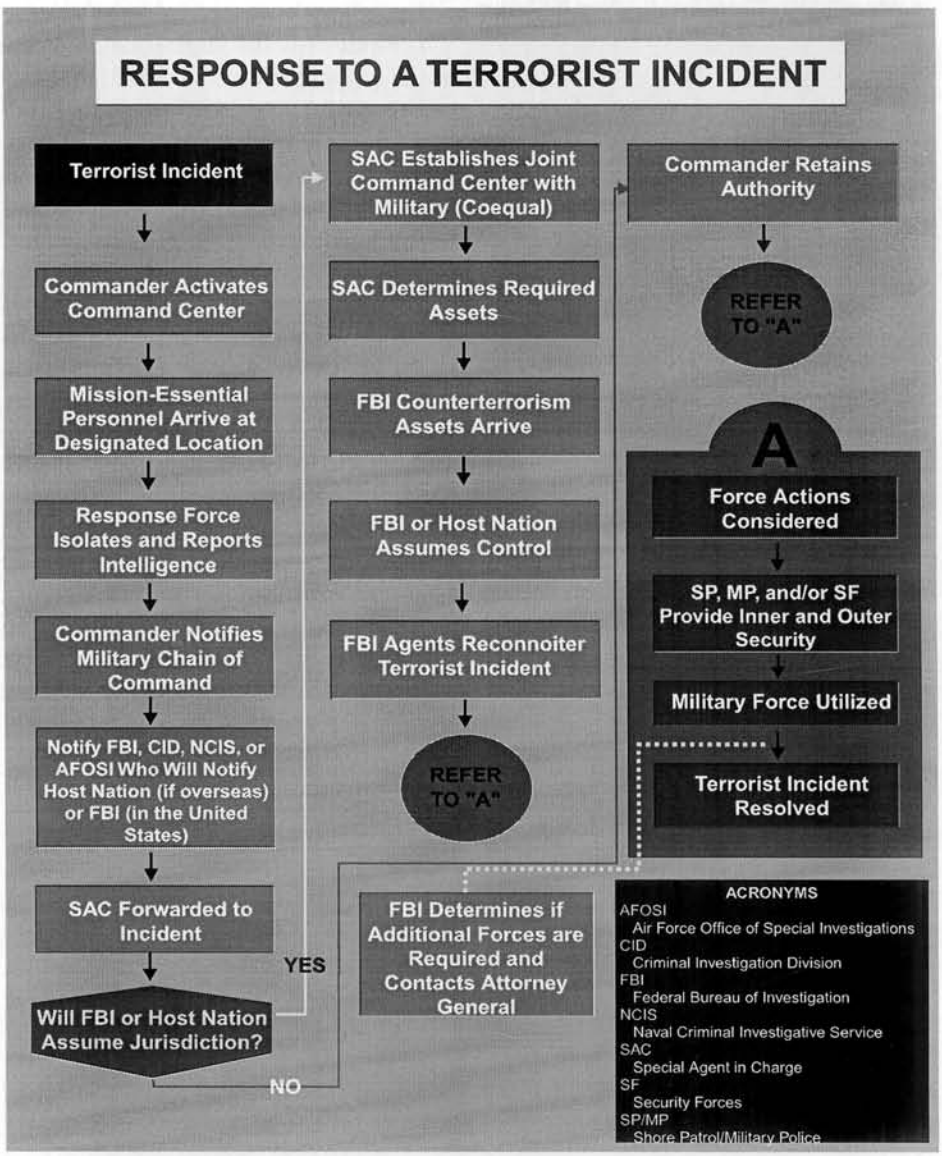


Figure VI-3. Response to a Terrorist Incident

4. Special Considerations

The following special considerations apply in implementing crisis management (See Figure VI-4).

a. **Establishing and Controlling Communications.** A crucial aspect of implementing the AT plan is **establishing and controlling secure communications among the forces in the incident area, the operations center, and the special response force**. The terrorists' communications with negotiators must also be established quickly and access to these communications must be limited. Once this is done, all other elements of the communications plan are activated. Communications personnel must be able to respond to changing needs during the incident and be able to maintain, over a prolonged period, control of all incoming and outgoing communications as well as the communications channels included in the AT plan.

b. **Evidence. Witness testimony and photographic evidence, for example, are important in achieving a successful prosecution.** Maintaining a continuous chain of custody on evidence obtained during an incident requires documenting the location, control, and possession of the evidence from

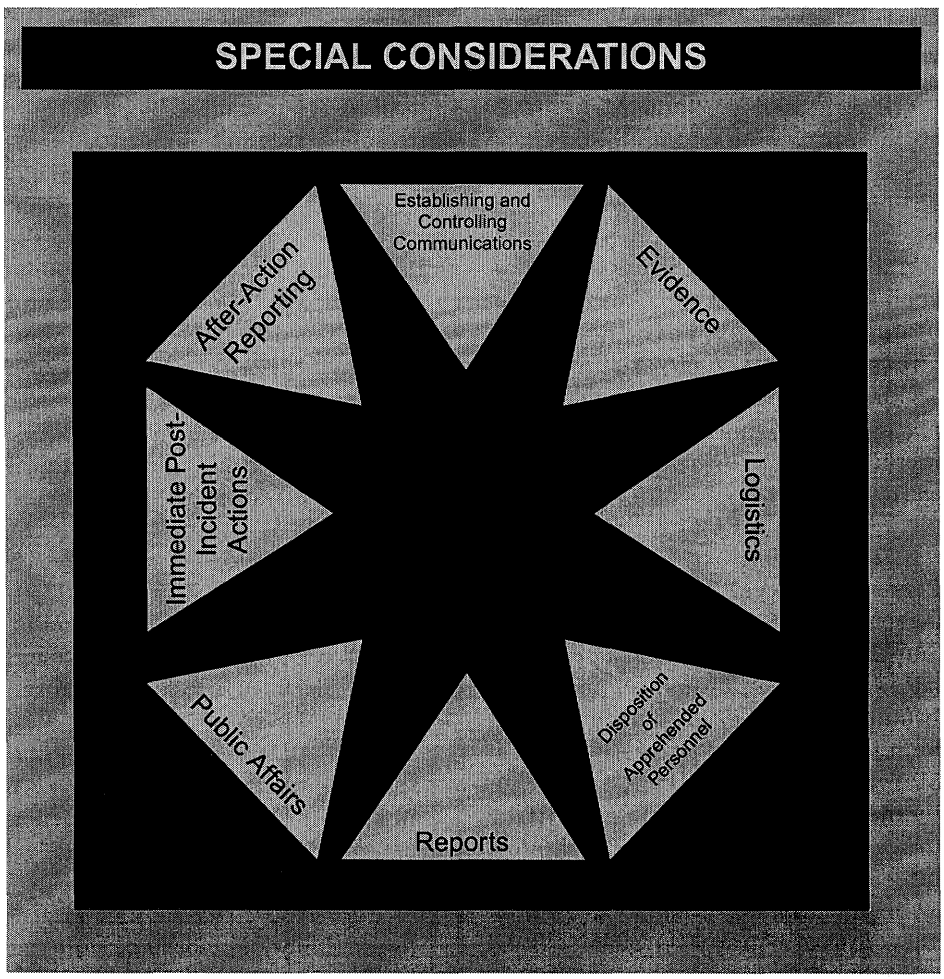


Figure VI-4. Special Considerations

the time custody is established until presenting the evidence in court. Failure to maintain the chain can result in exclusion of the evidence. Types of evidence for which the chain must be established include:

- Photographs and videotapes taken during the incident;
- Physical evidence, including any items used by the terrorists;
- Tape recordings of conversations between terrorists and hostage negotiators;
- Reports prepared by the military law enforcement authorities who initially responded to the incident scene;
- Eyewitness testimony; and
- Demand notes or other written messages prepared by the terrorists.

c. **Logistics.** An inherent responsibility for command authorities is the **consideration of logistics to support the special circumstances in a terrorist incident.** Shortages of communications equipment, photographic supplies, and vehicles, for instance, will reduce the capability of response and response forces.

d. **Disposition of Apprehended Personnel. Apprehended military personnel must be handled according to Service regulations and applicable installation, base, ship, unit, or port SOPs. In the United States, civilian detainees must be released to the FBI or US Federal Marshals for disposition. In foreign incidents, civilian detainees will be processed according to the SOFA, international agreement, or other arrangements with that particular country.** The command military legal authority should be consulted before releasing any individual to host-nation authorities.

e. **Reports. Reporting to higher headquarters is an important element in any special threat or terrorist situation.** Each Service and command should have 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. An after-action report should be prepared within 7 working days after termination of the event. This should include all staff journals and other documentation with detailed information concerning disposition of evidence and captured individuals. The command legal authority and military law enforcement personnel should ensure that this report is in sufficient detail to meet prosecution requirements.

f. **Public Affairs.** Principal public affairs objectives of an AT plan are to **ensure that accurate information is provided to the public (including news media) and to communicate a calm, measured, and reasonable reaction to the ongoing event.** Public affairs programs are designed to initiate the following:

- Identify terrorist activities as criminal acts not justifying public support.
- Reiterate US policy on terrorism, which identifies all terrorist acts as criminal acts, mandates no concessions to terrorists, refuses to pay ransom, and isolates those nations identified as fostering terrorism.
- Support DOD public affairs strategy on releasing information pertaining to AT plans, operations, or forces involved in antiterrorist operations.

  •• The DOJ has public affairs responsibility for incidents occurring on

US territory if the FBI assumes jurisdiction for resolving the incident.

•• When US military antiterrorist forces are employed, the Department of Defense provides a spokesman for dealing only with antiterrorist military operational matters. On military installations, the DOJ may delegate the public affairs responsibility to a designated DOD representative.

•• The DOS coordinates public affairs during terrorist incidents overseas. The DOS may delegate the public affairs responsibility to a designated DOD representative.

•• **The Office of the Assistant Secretary of Defense (Public Affairs) is the single point of contact for all public affairs aspects of US military antiterrorist actions.** Although there is no mandatory requirement to release information, installation commanders are advised to exercise prudent judgment on such matters.

•• When the operations center is activated, operations include the activities of the PAO and media center. The media center is located in a separate location from the operations center. The PAO is represented in both the operations center and media center and prepares media releases and conducts briefings at the media center during the incident, using information obtained by the PAO and cleared by the operations center and the commander. The PAO must be fully apprised of the situation as it develops. The media representatives should not have direct access to hostages, hostage takers, communications nets, or anyone directly involved in a terrorist incident unless the PAO has cleared such contact with the operations center. DOD experience with media representatives has shown that bringing them in early under reasonable conditions and restrictions commensurate with the risk and gravity of the event and providing them thorough briefings maintains DOD credibility and preserves freedom of information. Appendix M, "Public Affairs Checklist," provides additional guidance.

g. **Immediate Post-Incident Actions.** During the immediate post-incident phase, **medical and psychological attention (along with other support services) should be given to all personnel involved in the operation, including captured terrorists**. A final briefing should be given to media personnel; however, they should not be permitted to visit the incident site. 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 that every action that occurred during the incident be recorded.

h. **After-Action Reporting.** In the aftermath of a terrorist incident, **the operations center personnel review all the events and actions to revise the threat estimate, if necessary, and to determine the effectiveness of the AT plan**. All personnel involved in the AT operation should be debriefed and the debriefings recorded. This information will be used to develop lessons learned and after-action reports. It is the responsibility of the commander to ensure that all required after-action reports are prepared and subsequently reviewed with representatives of the command legal office. After-action reports should be submitted in accordance CJCSI 3150.25, "Joint After-Action Reporting System."

Intentionally Blank

CHAPTER VII
PREVENTIVE MEASURES AND CONSIDERATIONS

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

Attributed to Frederick the Great

1. Commander's Responsibility

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 deployment and expeditionary operations. Additionally, rest and recuperation (R&R) facilities 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, base, ship, unit, or port AT plan provides the mechanism to ensure readiness against terrorist attacks while the unit performs its tactical and technical mission during deployments. 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 in any situation.**

2. AT Force Protection in High-Risk Areas

The following are **antiterrorism tactics, techniques, and procedures for high risk missions**; they represent worst-case procedures. Security for forces performing security assistance, peacekeeping, mobile training teams, and other small military activities can be derived from these measures.

a. **Installations, Bases, Ships, Sites, and Non-Urban Facilities. Forces are frequently employed for security operations or other short-term, conventional, combat-related tasks.** Easily defended locations are often rare in urban areas because of building and population density or lack of proper cover and concealment and inability to create perimeter stand-off. Political restrictions may also limit the military's ability to construct fortifications or disrupt areas, but commanders must take all practical means to ensure force protection and identify shortcomings to appropriate levels of command for resolution. Military planners should adapt existing structures to provide protection based on the mission, potential for attack, and ability to use surroundings effectively.

- **Estimate of the Situation.** The commander and staff should complete a thorough estimate of the situation using mission, enemy, terrain, troops, time, and political planning factors in developing a security assessment. The following questions aid in developing an estimate of the terrorist situation:

  •• **Mission:** (1) Who is being tasked? (2) What is the task? (3) When and where is this task to take place? (4) Why are we performing this task?

  •• **Enemy:** (1) Who are the potential terrorists? (2) What is known about the terrorists? (3) How do the terrorists receive information? (4) How might the terrorists attack? (Think like the terrorists! Would you ambush or raid? Would you use snipers, mortars, rockets,

air or ground attacks, suicide attacks, firebombs, or bicycle, car, or truck bombs?) (5) Does your unit have routines? (6) What is the potential for civil disturbances and could terrorists use or influence these disturbances in an attack? Local law enforcement personnel (e.g., host-nation police) can at times be a valuable source for this information.

•• **Terrain:** (1) What are the strengths and weaknesses of the installation, base, ship, port, and local surroundings? (2) Are the avenues of approach above or below the water or ground? (3) Are there observation areas, dead spaces, fields of fire, illumination, or no-fire areas (e.g., schools)? (4) Are there tall buildings, water towers, or terrain either exterior or adjacent to the perimeter that could become critical terrain in the event of an attack?

•• **Troops:** (1) Determine what is the friendly situation. (2) Are other US forces or equipment available? (3) Are engineers and/or EOD in the area? Will they be able to provide support? (4) Are emergency reinforcements available? (5) Are MWD teams available? (6) What are the host-nation responsibilities, capabilities, and attitudes toward providing assistance? (7) What restraints will be imposed by the US Government on the show or use of force?

•• **Time:** (1) What is the duration of the mission? (2) Are there time constraints? (3) Will there be sufficient time to construct force protection facilities such as barriers, fences, and lights?

•• **Political Planning Factors:** (1) Are there host-nation concerns or attitudes that will impact on the situation? (2) Will the situation be influenced by the existence of any religious or racial concerns?

- **Develop Plan.** Defenses should include a combination of law enforcement and security assets, fortifications, sensors, obstacles, local-hire security forces (if applicable), unit guards, deception, and on-call support from reaction forces. **Each situation requires its own combination of abilities based on available resources and perceived need.** Figure VII-1 provides general guidance concerning fortification materials.

•• **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. 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.

•• **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 law enforcement personnel.

FORTIFICATION MATERIALS		
FORTIFICATION	MATERIAL	PURPOSE
Wire fences	Barbed wire Concertina wire Chain link/weld mesh	Delay access Channel movement through manned points Use as grenade, firebomb, or high explosive antitank rocket barriers
Screens	Canvas Plywood Natural growth	Deny observation inwards (Note: may also prevent observation outwards. Additional sensors may be required.)
Canopies	Chain link/weld mesh Corrugated iron	Protect roofs Detonate mortar projectiles Absorb shrapnel Cover machineguns positioned on roofs
Sandbags	Sandbags	Absorb shrapnel Protect personnel and equipment
Sensors and Closed Circuit TV		Provide early warning

Figure VII-1. Fortification Materials

Security forces should have available to them and be trained in specialized equipment for responding to terrorist attacks and/or incidents (See Figure VII-2). Local installations, with the assistance of the parent Service, should identify and procure this equipment based on Service directives and the local situation.

- **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:

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

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

SECURITY FORCE EQUIPMENT	
Pyrotechnic pistols	Marshalling wands
Riot shotguns	Telescopes and tripods
Tear gas launchers	Binoculars
Hand-held flashlights	Night vision devices
Antiriot helmets	Loud speakers
Shields 3'6"	Fire extinguishers
Shields 6'	Cameras with flash and tripods
Side-handled or straight batons	Telescopic sights
Hand cuffs	Photographic filter
NBC protective masks	Body Armor

Figure VII-2. Security Force Equipment

•• Establish inspections and immediate action drills, exercises, and training to implement the security plan.

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

•• Keep abreast of current military and host-nation police and intelligence assessments.

b. **Guard Duties.** Guard duties are detailed in Service regulations and in local, general, and special orders. In a terrorist high-risk environment, special orders should address as a minimum the following:

- Details of authorized passes; provide samples of passes.
- Procedures for searching people and vehicles.
- Response to approach by unauthorized personnel or hostile crowds.
- Specific rules of engagement (ROE) or use of force policy in the event of civil disturbances, potential damage, or injury to US personnel or specific property, looting, or arson.
- Response to unauthorized photography and surveillance activities.
- Steps necessary to obtain police, reaction force(s), fire department, and ambulance.
- Guidelines for contact with host-nation police.
- Guidelines for contact with press and media.

c. **Road Movement.** Road movements are always vulnerable to terrorists 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:

- Avoid establishing a regular pattern;
- Vary routes and timing;
- Travel in groups, never single vehicles;
- 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);

- When possible, keep a low profile (use vehicles that do not stand out);
- Plan alternate routes and reactions to various threatening scenarios;
- Plan communications requirements;
- Avoid dangerous areas (e.g., ambush sites, areas known for violence);
- Provide adequate security;
- Plan in advance for maintenance and evacuation; and
- Use countersurveillance.

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

- Place sandbags on floorboards and fenders.
- Cover sandbags with rubber or fiber mats.
- If carrying personnel, sandbag the vehicle bed as well as the driver's compartment.
- Remove canvas so passengers can see and shoot.
- Fold windshield in driver's compartment and fit high-wire cutter. Lower side windows and place wire over all openings to deflect grenades or IEDs.
- Normally, avoid large concentrations of personnel in any one vehicle. If necessary, assign convoys additional vehicles to disperse personnel loads.
- Passengers riding in truck bed face outboard and are assigned sectors of observation and fire.
- Rig chicken wire or chain link screens on front bumper frame to deflect rocks, bottles, firebombs, and grenades.
- Carry pioneer tools (fire extinguishers in particular), a line with grappling hook to clear obstacles, and tow bars for disabled vehicles.
- When the threat of hostile fire is constant, plan for the use of vehicles with additional armored protection.

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

- Develop and rehearse immediate action drills before movement.
- Perform route clearance before movement.
- Establish and maintain communications throughout the route.
- Develop deception plans to conceal or change movement timing and route.
- If possible, include host-nation police and/or military personnel in the convoy.
- When selecting routes, avoid entering or remaining in dangerous areas. If ambushed, gauge response by enemy strength. Counter ambushes by accelerating through the ambush area, counterattacking, withdrawing, or withdrawing and staging a deliberate attack.

- Convoy escort composition depends on available forces. Light armored vehicles, high mobility multipurpose wheeled vehicles, or trucks equipped with M2 50-caliber and MK19 40mm machine guns are extremely effective. Overhead helicopters and AC-130 gunships can also be used as air escorts if available. Escorts should be organized into an advance guard, main body escort, and reaction or strike group. Planning considerations are as follows:
  - •• Determine concept of operation.
  - •• Identify available transportation.
  - •• Identify order of march and road organization.
  - •• Identify disposition of advance guard, main body escort, and reserve.
  - •• Designate assembly area for convoy.
  - •• Determine rendezvous time at assembly area, departure time of first and last vehicle, and expected arrival of first and last vehicle at destination.
  - •• Identify action upon arrival.
  - •• Determine required coordinating instructions for speed, spacing, halts, immediate action drills, breakdowns, and lost vehicles.

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

- Restrict passengers to military personnel only.
- Search for explosives or possible hijackers before departure and after every halt (MWDs are particularly suited for this mission). Appendix N, "Military Working Dogs," provides information concerning use of MWDs in antiterrorism operations.
- Ensure that the railway is free of obstructions or explosives.
- Patrol the railway area.
- Place armed security personnel on duty throughout the train, including engine room and trail car.
- Patrol and guard departure and arrival stations.
- Use deception measures.
- Provide air cover (AC-130, helicopters).
- Maintain communications within the train and with outside agencies.
- Provide reaction force to be moved by air or coordinate host-nation support (HNS) (if available).

g. **Sea Movement. Sea movement, especially aboard military vessels, may provide a false sense of security.** Sea operations are certainly more secure than urban patrols; **however, ships in harbor or anchored off hostile coastlines are visible and high-risk targets.** Crews of ships in harbors need to evaluate each new port and determine possible terrorist actions and ship's force counteractions (such as using fire and steam hoses to repel attackers). Crew members must be aware of HNS and responsibilities while in port or anchored in foreign national waters. **The ship's captain is solely responsible for the ship and all those embarked.** As a minimum, the captain:

- Establishes methods of embarkation and debarkation and patrol activities for all personnel;
- Identifies vital areas of the ship (for example, engine room, weapons storage, command and control bridge), and assigns security guards;
- Coordinates above and below waterline responsibilities;
- Establishes a weapons and ammunition policy and ROE, and appoints a reaction force (e.g., security alert team [SAT], backup alert force [BAF], and/or reserve force [RF]); and
- Drills all personnel involved.

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

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

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

j. **Roadblocks. There are two types of roadblocks: deliberate and hasty. Deliberate roadblocks** are permanent or semipermanent roadblocks used on borders, outskirts of cities, or the edge of controlled areas. Use deliberate roadblocks to check



Deployed joint forces may be tasked to conduct antiterrorist operations in urban areas.

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

k. **Observation Posts. OPs provide prolonged observation of areas, people, or buildings.** OPs are critical. 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, and using deception. Any compromise of an OP location should be immediately reported.

l. **Civil Disturbances. Crowd violence can either be a spontaneous emotional eruption or a planned event.** In the latter case, its purpose is to draw police or troops into a target area or away from some other event. Crowd violence may also involve violence within the crowd or from opposing groups. Crowd violence is characterized by incitement and violence; both are highly contagious. Riot control aims to restore order with minimum use of force. Bearing in mind that the size or motivation of the crowd may

prevent its control, the general approach is to reduce or disrupt the crowd's unifying influences and reorient the participants to concerns for personal vulnerability and welfare. The principles of riot control are shown in Figure VII-3.

m. **Bomb Explosion or Discovery. The initial terrorist bomb may not be the end of the incident.** The initial bomb may be designed to draw forces into an area as targets for a shooting ambush or another explosion. Upon discovery of a bomb or upon entering a bomb site, response forces should proceed with extreme caution and contact the EOD team immediately. MWDs or explosive detection dogs should be considered upon bomb discovery or during entry to the site of the explosion. Appendix K, "Explosive Device Procedures," contains procedures for handling bomb situations.

PRINCIPLES OF RIOT CONTROL

1. Flexibility in changing tactics as necessary to meet the situation
2. Rehearsals ensure success
3. The appearance of being able to do damage is often more effective than actually having to resort to force
4. Control the situation by positioning personnel and presenting the image of having and maintaining full control even if the situation deteriorates
5. Provide all-round defense of assigned sectors of observation and fire and be able to observe and fire 360 degrees around control force
6. There must be speed in deployment, arrest, and apprehension, and reaction to change
7. Surprise keeps the crowd off balance

Figure VII-3. Principles of Riot Control

n. **Personal Protective Measures. Overseas deployments require a high degree of personal protective measures.** The guidelines in Appendix B, "Personal Protective Measures Against Terrorism," still apply, 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 law enforcement and intelligence agencies and host-nation forces is critical. The deployed military member must also understand the threat and required personal security measures.

3. Tactical Force Protection

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

Intentionally Blank

APPENDIX A
VULNERABILITY ASSESSMENT

1. General

The VA provides the commander with a tool to assess the potential vulnerability of a base, unit, ship, or port activity, but it is not a substitute for sound judgment. These guidelines also serve to limit the scope of the force protection vulnerability assessments to those elements that are **directly and uniquely related to combatting terrorism** and are only one part of the larger issue that clearly and appropriately belongs to the traditional commanders' responsibilities for the overall well-being of Service members, civilian employees, and family members as well as facilities and equipment. The VA must stand on its own and be supported by valid considerations. Typically, a small group of knowledgeable individuals (at the minimum operations, law enforcement, security, intelligence, counterintelligence, communications, engineer staff, medical services, housing, fire protection, emergency planning, and NBC defense and response) develop the VA and forward it to the command group upon completion. The command group then uses the VA as an aid in developing measures to counter the threat.

2. Assessing Vulnerability

It is understood that each location, site, or facility is unique in terms of vulnerability to terrorist operations. Accordingly, these guidelines are intended to be flexible, allowing for adaptation to site circumstances.

a. **Functional Areas.** The concept for force protection VA is to focus on two broad areas:

- Preventing and, failing that, substantially mitigating the effects of a terrorist act.
- Emergency preparedness and crisis response.

Combined, the proactive and the reactive capabilities within these two broad areas form the essence of what can be considered the essential elements for deterring and combatting terrorism.

b. The proactive and reactive aspects of force protection are divided into four significant elements:

- **Physical security.** Consists of all the functional areas that make up those measures necessary to protect and safeguard personnel, facilities, and installations from terrorist acts.
- **Weapons effect mitigation.** Consists of all the functional areas that make up the capability to calculate blast, shock, shrapnel, fire, and other damage associated with chemical explosives; to calculate effects from other weapons that terrorist might employ including WMD; and to assess the mitigating values of standoff distances, blast barriers, structural hardening, and a host of adjunct mitigating capabilities, including emergency preparedness and response capabilities.
- **Threat, vulnerability, and risk analysis.** Consists of the functional areas that make up the capability to assess how well the threat statements produced by the intelligence community (DIA, CINC J-2, Service, national, local intelligence authorities, and local unit level) have been fused with logical analysis and conclusions about terrorist abilities to attack a specific installation, facility, or

group of people. Consistency of produced threat estimates, reasonably postulated terrorist target and target vulnerability estimates, and efforts to enhance security and reduce weapons effects are major functions in this element.

- **Application of DOD standards.** To the extent that the DOD standards for force protection go beyond the functional expertise required to do the first three force protection elements, the requisite expertise may be collected by the installation, base, ship, unit, or port activity in this area. The standards' compliance area is more an assessment of the vulnerability reduction value of the standards than it is a review to determine if the standards are being complied with.

3. Areas of Expertise

Required areas of expertise for a VA team.

a. **Assessment Team Chief.** Key responsibilities: Overall management, training, and performance of the vulnerability team members; finalizing the assessment team out-briefing; preparing the population dynamics and risk assessment.

- Ensures that the team is properly trained, prepared and equipped.
- Ensures that the team members have the appropriate security clearances.
- Oversees the pre-deployment collection and analysis of available information to support the deployment.
- Oversees operational and procedural security training for team members.
- On-site, assesses critical population centers and mass population areas including travel routes; assists in threat and vulnerability analysis.

b. **Physical Security Specialist.** Key Responsibilities: Installation, facility, and personnel security and safety. Major functions performed:

- Assess overall physical security, operations, and information security.
- Assess access control, to include sensors and intrusion devices.
- Assess perimeter defensive positions and vehicular and/or personnel barriers.
- Assess lighting, police security, and security response planning and force capability.
- Assess overall security planning and responsiveness to threat assessments and prepared intelligence estimates.
- Assess relationship and support from local law enforcement and other security agencies, both local and national.
- To the extent that vulnerabilities are found, formulate and suggest mitigating measures and assist in their implementation.

c. **Structural Engineer.** This function examines a variety of potential terrorist weapon effects and structural responses in order to better protect personnel from shock and blast by reducing damage through technically appropriate use of stand off measures, hardening, blast shielding, and shatter-resistant window film (i.e., mylar). Key responsibility: Threat and damage assessment from terrorist weapons estimates; suggestions for threat protection or damage mitigation measures. Major functions performed:

- Assess damage mechanisms including blast, shock, and fragmentation. Calculate hazardous radii based on structural dynamics and calculated structural loads.

- Assess building and barrier resistance or mitigation of threat weapons effects. Determine appropriate standoff distance, potential hardening or other mitigating measures.

- Assess systems related to physical security and personnel protection (warning devices, alarms).

- Assess and/or identify safe havens.

- Assess mechanical, electrical, and other service systems for vulnerability to weapons effects and suggest mitigating measures.

- To the extent that structural vulnerabilities are found, formulate and suggest mitigating measures and assist in their implementation.

d. **Infrastructure Engineer.** This function examines three distinct elements of force protection:

- Protection against the effects of WMD.

- Protection against terrorist incident-induced fires.

- Utility systems that can be employed to minimize terrorist incident casualties, including elements of power, environmental control, and life support systems. Key responsibilities: Infrastructure security, fire, safety, and damage control. Major functions include:

•• Assess facility and operational utility systems for susceptibility to damage from terrorist acts.

•• Assess fire protection planning and capabilities, including emergency response planning and exercises.

•• Assess vulnerability of installation utilities and plans for back-up services.

•• Assess availability of support, to include use of local national capabilities.

•• Assess mechanical, electrical, and other infrastructure systems for vulnerability to weapons effects and suggest mitigating measures.

•• To the extent that structural vulnerabilities are found, formulate and suggest mitigating measures and assist in their implementation.

e. **Operations Readiness Specialist.** This function examines plans, procedures and capabilities for crisis response, consequence management, and recovery operations, should a terrorist incident occur. The operations readiness objectives are to provide individual protective measures and emergency response capabilities that minimize mass casualties and reduce the number of severe injuries and fatalities. Operational readiness includes training of all personnel in response actions to tactical warning, alarms of imminent attack, planning and exercise of rescue operations, emergency medical triage, and treatment in mass casualty situations. The installation's Force Protection and/or Antiterrorism officer, the installation fire chief, emergency medical services, and local and/or host country fire and medical services all play a part in force protection operations readiness. Key

responsibility: Emergency medical and individual readiness assessments. Major functions performed:

- Assess individual, personnel, facility, and installation protection capabilities.
- Assess emergency medical capabilities and planning including the identification of key assets and infrastructure.
- Assess recovery procedures and planning to understand the ability to recover from loss of key assets, infrastructure, or facilities.
- Assess planning and/or consideration of evacuation as a risk mitigating measure.
- Assess application of the DOD force protection standards and determine their value in vulnerability reduction.
- To the extent that structural vulnerabilities are found, formulate and suggest mitigating measures and assist in their implementation.

f. **Intelligence and/or Counterintelligence Specialist.** Key responsibility: Performs logical analysis and prepares possible conclusions regarding terrorist targets and target vulnerabilities based on processed intelligence information, knowledge of terrorist capabilities, and methods and in view of US installation, facility, and personnel safety and security practices. Major functions performed:

- Develop possible threat scenarios.
- Assess installation, facility, and personnel vulnerability in view of scenarios, and in consideration of ongoing counterintelligence activity, demonstrated capabilities in exercises, capabilities of local authorities, and terrorist intelligence activities.
- Propose additional security, counteraction, and threat reduction efforts.

g. Communications, housing, fire protection, NBC defense, and response are functional areas which can be executed by any team member if appropriate for the mission and threat of the installation, base, ship, unit, or port activity.

4. Assessment Planning, Preparations and Conduct

This section addresses the activities which may be performed in order to provide a force protection VA visit and upon completion of the visit.

a. **Pre-assessment Preparations.** The key element of preparation is the beginning of the site folder development. The site folder is the official record of the assessment team information gathering, analysis, recommendations, and assistance for the commander. A critical aspect of the site folder formation is the intelligence information gathering relative to the terrorist threat. All-source intelligence on groups, motivation and intent, tactics and weapons, activities, and operating areas should be obtained from DIA, CINC J-2, and other sources. A complete list of installation characteristics, including layouts, drawings, functions, personnel, and procedures, should be requested in advance of the visit to be sent to the requesting team or made available upon arrival. If available, a copy of the antiterrorism plan may be made available to the assessment team.

- Administrative preparations include coordination particulars of the visit with the installation, base, ship, unit, or port activity, including:
  - Theater clearances (if applicable).
  - Requirements for invitational travel orders, passports, visas, inoculations,

insurance (health life) and other legal issues as well as emergency information forms.

- Security preparations include:
  - •• Identifying a security representative.
  - •• Submitting requests for country clearances and identifying classified documents to be couriered.
  - •• Coordinating secure storage for arrival.
  - •• Preparing letter requests for overseas courier authorization.
  - •• Presenting mandatory threat briefing and mandatory security procedures briefing
- Logistics preparations include:
  - •• Any travel arrangements (tickets, lodging, and billeting).
  - •• Travel kits (pharmaceuticals and supplies).
  - •• Equipment checkout and packaging and shipping.

b. **Conduct of the Assessment.** Upon arrival, the assessment team provides an in-briefing for the commander, staff, and designated technical point of contact. A site familiarization briefing and tour should be conducted by site personnel. Administrative activities may include establishing the team support area, setting up equipment, scheduling team and/or technical points of contact meetings and discussions, ensuring classified material control, establishing personnel locator, and organizing materials (view graph, photos, and diagrams) for the out-briefing and site folder. Each assessment team member conducts the assessment based on the specific responsibilities for each functional area as outlined above.

c. **Post-assessment Activities.** Within 30 days of the conclusion of the visit, a summary narrative report and annotated briefing should be delivered to the installation commander. Follow-on assistance for the commander may be applicable in areas of technical characteristics of improvement options, cost estimates, and generic sources of materials and equipment. Lessons learned from the assessment should be extracted and entered in the Joint Universal Lessons Learned System.

Intentionally Blank

APPENDIX B
PERSONAL PROTECTIVE MEASURES AGAINST TERRORISM

1. General

Any member of the Department of Defense — not just senior leaders — can become a target for terrorists. The purpose of this appendix is to provide general guidance to DOD members and their families on how to avoid acts of terrorism, as well as to provide basic instructions in the event DOD personnel become victims of a terrorist attack.

2. Precautions

Since terrorist acts are criminal acts, measures taken to protect oneself from terrorism are similar to those measures taken to guard against crime. Attitude toward security is most important. Although some of these precautions are applicable overseas, you can decrease your chances of becoming a terrorist target, as well as those of your family members, by taking the precautions listed in this appendix. Therefore, it is highly recommended that you share this information with every member of your family. It is also suggested that you and your family review these precautions on a regular basis.

a. **At All Times**

- Encourage security awareness in your family and discuss what to do if there is a security threat.
- Be alert for surveillance attempts or suspicious persons or activities, and report them to the proper authorities. Trust your gut feelings.
- Vary personal routines whenever possible.
- Get into the habit of checking in to let your friends and family know where you are or when to expect you.
- Know how to use the local phone system. Always carry telephone change. Know the emergency numbers for local police, fire, ambulance, and hospital.
- Know the locations of civilian police, military police, government agencies, US Embassy, and other safe locations where you can find refuge or assistance.
- Avoid public disputes or confrontations. Report any trouble to the proper authorities.
- Know certain key phrases in the native language such as "I need a policeman," "Take me to a doctor," "Where is the hospital?," and "Where is the police station?"
- Set up simple signal systems to alert family members or associates that there is a danger. Do not share this information with anyone not involved in your signal system.
- Carry identification showing your blood type and any special medical conditions. Keep a minimum of a 1-week supply of essential medication on hand at all times.
- Keep a low profile. Shun publicity. Do not flash large sums of money.
- Do not unnecessarily divulge your home address, phone number, or family information.

- Watch for unexplained absences of local citizens as an early warning of possible terrorist actions.
- Keep your personal affairs in good order. Keep wills current, have powers of attorney drawn up, take measures to ensure family's financial security, and develop a plan for family actions in the event you are taken hostage.
- Do not carry sensitive or potentially embarrassing items.

b. **At Home**

- Have a clear view of approaches to your home.
- Install strong doors and locks.
- Change locks when you move in or when a key is lost.
- Install windows that do not allow easy access.
- Never leave house or trunk keys with your ignition key while your car is being serviced.
- Have adequate lighting outside your house.
- Create the appearance that the house is occupied by using timers to control lights and radios while you are away.
- Install one-way viewing devices in doors.
- Install intrusion detection alarms and smoke and fire alarms.
- Do not hide keys or give them to very young children.
- Never leave young children at home alone.
- Never admit strangers to your home without proper identification.
- Use off-street parking at your residence, if at all possible.
- Teach children how to call the police, and ensure that they know what to tell the police (e.g., name, address).
- Avoid living in residences that are located in isolated areas, on one-way streets, dead-end streets, or cul-de-sacs.
- Avoid residences that are on the ground floor, adjacent to vacant lots, or on steep hills.
- Carefully screen all potential domestic help.
- Do not place your name on exterior walls of residences.
- Do not answer the telephone with your name and rank.
- Personally destroy all envelopes and other items that reflect personal information.
- Close draperies during periods of darkness. Draperies should be opaque and made of heavy material.
- Avoid frequent exposure on balconies and in windows.
- Consider owning a dog to discourage intruders.
- Never accept unexpected package deliveries.
- Don't let your trash become a source of information.

c. **While Traveling**

- Vary times and routes.
- Be alert for suspicious-looking vehicles.
- Check for suspicious activity or objects around your car before getting into or out of it. Do not touch your vehicle until you have thoroughly checked it (look inside it, walk around it, and look under it).
- Know your driver.
- Equip your car with an inside hood latch and a locking gas cap.
- Drive with windows closed and doors locked.
- Travel with a group of people — there is safety in numbers.
- Travel on busy routes; avoid isolated and dangerous areas.
- Park your car off the street in a secure area.
- Lock your car when it is unattended.
- Do not routinely use the same taxi or bus stop. NOTE: Buses are preferred over taxis.
- If you think you are being followed, move as quickly as possible to a safe place, such as a police or fire station.
- If your car breaks down, raise the hood then get back inside the car and remain there with the doors locked and the windows up. If anyone offers to assist, ask the person to call the police.
- Do not pick up hitchhikers.
- Drive on well-lit streets.
- Prearrange a signal with your driver to indicate that it is safe to get into the vehicle. Share this information only with persons having a need to know.
- Have the driver open the door for you.
- If the driver is absent, do not get into the car.
- If possible, tell your driver your destination only after the car has started.
- Keep your vehicle's gas tank at least half full.

d. **In Hotels**

- Keep your room key on your person at all times.
- Be observant for suspicious persons loitering in the area.
- Do not give your room number to strangers.
- Keep your room and personal effects neat and orderly so you will recognize tampering or strange out-of-place objects.
- Know the location of emergency exits and fire extinguishers.
- Do not admit strangers to your room.
- Know how to locate hotel security guards.

e. **Ground Transportation Security**

- Use a plain car that is common in the area to minimize the rich American look.
- Do not be predictable in your daily travel behavior; vary your travel times, your

routes, and your mode of transportation whenever possible.

- Check the area around the vehicle, the exterior of the vehicle, and then the interior of the vehicle before starting the engine.
- Travel with companions or in convoy whenever possible.
- Know the locations of safe havens (e.g., police and fire stations) along your travel routes.
- Install appropriate mirrors, locks, and other devices to secure your car against tampering.
- Safeguard car keys at all times.
- Screen chauffeurs or permanently assigned drivers. Develop a simple system for the driver to alert you to danger when you are picked up. Share this information only with persons having a need to know.
- Lock your car, especially at night, and check and lock your garage when you park there overnight.
- Park in well-lighted areas if you must park on the street.
- Always fasten seat belts, lock doors, and close windows when driving or riding in a car.
- Be alert for surveillance and be aware of possible danger when driving or riding in a car.
- Drive immediately to a "safe haven" when surveillance is suspected; do not drive home.

f. **Air Travel Security**

- Use military aircraft whenever possible.
- Avoid travel through high-risk areas; use foreign flag airlines and/or indirect routes to avoid such areas.
- Do not use rank or military addresses on tickets, travel documents, hotel reservations, or luggage.
- Select a window seat on aircraft because they offer more protection and are less accessible to hijackers than are aisle seats.
- Select a seat in the midsection of the aircraft because it is not one of the two usual areas of terrorist activity.
- Do not discuss your US Government affiliation with any other passengers.
- Consider using a tourist passport when traveling in high-risk areas; if you use a tourist passport, store your official passport, identification card, travel orders, and other official documents in your carry-on bags. Also, if you normally wear a military ring (e.g., Service or academy), consider leaving it at home or pack it in your checked baggage.
- Do not carry classified material unless it is mission-essential.
- Use plain civilian luggage; avoid using B-4 bags, duffel bags, and other military-looking bags. Remove all indications of your rank and any military patches, logos, and decals from your luggage and briefcase.
- Do not carry official papers in your briefcase.
- Travel in conservative civilian clothing. Do not wear military-oriented organizational shirts or caps or military-issue shoes or glasses. Also, avoid

obvious American clothing such as cowboy boots and hats as well as American-logo T-shirts. Cover visible US-affiliated tattoos with a long-sleeved shirt.

- If possible, check your baggage with the airport's curb service.

- Adjust your arrival at the airport to minimize waiting time, be alert for any suspicious activity in the waiting area, and proceed immediately to the departure gate.

3. Hostage Defense Measures

a. Survive with honor — this is the mission of any American hostage.

b. If your duties may expose you to being taken hostage, make sure your family's affairs are in order to ensure their financial security. Make an up-to-date will and give appropriate powers of attorney to your spouse or to a trusted friend. Concern for the family is a major source of stress for persons in kidnap or hostage situations.

c. If you are taken hostage and decide not to resist, assure your captors of your intention to cooperate, especially during the abduction phase.

d. Regain your composure as quickly as possible after capture, face your fears, and try to master your emotions.

e. Take mental note of the direction, time in transit, noise, and other environmental factors that may help you identify your location.

f. Note the numbers, names, physical characteristics, accents, personal habits, and rank structure of your captors.

g. Anticipate isolation and terrorist efforts to confuse you.

h. Try to mentally prepare yourself for the situation ahead as much as possible. Stay mentally active.

i. Do not aggravate your abductors; instead, attempt to establish a positive relationship with them. Do not be fooled by a friendly approach — it may be used to get information from you.

j. Avoid political or ideological discussions with your captors; comply with their instructions, but maintain your dignity.

k. Do not discuss or divulge any classified information that you may possess.

l. Exercise daily.

m. Read anything you can find to keep your mind active.

n. Eat whatever food is offered to you to maintain your strength.

o. Establish a slow, methodical routine for every task.

p. When being interrogated, take a simple, tenable position and stick to it. Be polite and maintain your temper. Give short answers, talk freely about nonessential matters, but be guarded when the conversation turns to substantial matters.

q. If forced to present terrorist demands to authorities, in writing or on tape, do only what you are told to do. Avoid making a plea on your own behalf.

r. Be proud of your heritage, government, and military affiliation, but be careful that your behavior does not antagonize your captors. Affirm your faith in basic democratic principles.

s. In the event of a rescue attempt:

- Drop to the floor. Do not move unless instructed to do so by the rescuing force. Under no circumstances attempt to assist the rescue force. Stay completely clear of anything that could be regarded as or misidentified as a weapon;
- Be quiet and do not attract your captors' attention;
- Wait for instructions;
- Rescue forces will initially treat you as one of the terrorists until you are positively identified as friend or foe. This is for your security. Cooperate, even if you are initially handcuffed or bound; and
- Once released, do not make comments to the news media until you have been debriefed by the proper US authorities and have been cleared to do so by the appropriate military commander.

APPENDIX C
VERY IMPORTANT PERSON AND SENIOR OFFICER SECURITY MEASURES

1. General

Very important persons and senior officers are terrorist targets by virtue of their position and symbolic nature. Although the level of threat to these individuals varies, their best protection is their own awareness of this threat as well as their dependents' awareness of the threat. The following measures are steps that they can take in their daily activities to reduce their exposure to terrorist attacks.

2. Security at Home

a. Evaluate home security requirements.

b. Check persons entering the premises (e.g., electricians, plumbers, telephone maintenance personnel). If in doubt, call their office to verify their identity before allowing them in your home.

c. Do not open the door to a caller at night until the caller is identified by examination through a window or door viewer.

d. Ensure that all door locks and window clasps are working.

e. Consider installing a door security chain, spyglass, or visitor intercom.

f. Consider locking the driveway gates with a security lock to prevent entry.

g. Consider installing security lights to aid in viewing entrances.

h. Close curtains in a room before turning on lights.

i. Consider fitting windows with either venetian blinds or thick curtains.

j. Have reserve lighting handy (e.g., flashlight, lamps).

k. Consider placing the telephone where you will not be seen from doors or windows when answering.

l. Investigate household staff (especially temporary staff).

m. Always be on the lookout for the unusual. Ensure that home is locked and secure whenever the residence is unattended. Be cautious upon return.

n. Note and report suspicious persons.

o. Strictly control house keys.

p. Place car in a locked garage.

q. Be alert for the unusual (e.g., the movement of furniture or the placing of unusual wires).

r. Consider the fitting of a panic alarm bell to the outside of the house with switches upstairs and downstairs.

s. Clear the area around the house of dense foliage or shrubbery.

t. Test your duress alarm if available. Make certain the members of your family understand the importance of the alarm and how it works.

u. Cooperate with law enforcement personnel and abide by their security

recommendations concerning your home's security.

3. Security To and From Work

a. Vary your daily pattern as much as possible. Leave and return at different times. Use alternative routes, but notify your office of chosen route prior to departure.

b. Be discreet in forecasting movements, but ensure that someone knows your whereabouts at all times.

c. Consider traveling to and from work with escorts, or travel with a neighbor.

d. Use defensive and evasive driving techniques. Drill with your driver by watching for suspicious cars and taking evasive action.

e. Keep car doors locked. Do not open windows more than a few inches.

f. Park car in a safe area.

g. Keep the trunk locked. Never leave large bulky items in the trunk of unattended parked cars that would prevent locking the trunk.

h. Examine car before entering to see if there has been any interference. A small mirror on a rod is a cheap and effective method to inspect underneath cars. Do not touch the vehicle until it has been thoroughly checked (look inside it, walk around it, and look under it).

i. Do not leave personal items exposed in the car (e.g., uniform items, Service-issued maps, official briefcases).

j. Use the same precautions when you drive a privately owned vehicle.

4. Security at Official Functions

a. Discuss security requirements with the person planning the function.

b. Travel to and from the function with escorts.

c. Choose the route carefully.

d. Do not publicize planned attendance at official functions unless required.

e. Attempt to sit away from both public areas and windows.

f. Encourage the sponsor(s) of the function to close the curtains to minimize the likelihood that anyone outside will be able to see inside and determine who is attending the function and where they are located. This is extremely important for an evening function, when a well-lit interior can be easily viewed from outside.

g. Request external floodlights be used to illuminate the area around the building where an evening function will occur.

5. Security at Private Functions

a. Ensure that the host is aware of your need for security and takes appropriate measures.

b. Have your personal staff assist a civilian host if required.

c. Arrange for visitors to be subject to adequate security control.

d. Screen the invitation list, if possible.

e. Vary times of sporting activities (e.g., golfing, jogging).

6. Security During Travel

a. Book airline seats at the last moment. Consider using an alias.

b. Restrict the use of rank or title.

c. Do not allow unknown visitors in hotel room or suite.

d. Keep your staff and your family members advised of your itinerary and subsequent changes. Restrict this information to those having a need to know.

7. Security of Children

a. Ensure children's rooms are not readily accessible from outside the house.

b. Instruct children never to admit strangers to the house.

c. Teach children when and how to alert police or neighbors.

d. Instruct children attending school to travel in groups or at least in pairs, use busy thoroughfares, and avoid play areas outside the school.

e. Instruct children to refuse gifts or approaches from strangers.

f. Instruct children to immediately report attempts of an approach to the nearest responsible adult, and also to tell you as soon as possible.

g. Instruct children to tell you where they are, who they are with, and how long they will be away from the house.

h. Instruct children not to discuss what you do and to tell you if they are questioned about you by anyone.

i. Encourage children to report suspicious incidents to you.

j. Accompany young children to and from bus stops, where necessary.

k. Do not allow preschool children to wander from the house or play in areas where they cannot be supervised.

l. Discourage children from answering the door, especially during hours of darkness.

m. Advise children attending schools away from home to use the applicable techniques listed above in their daily activities.

Intentionally Blank

APPENDIX D
BUILDING SECURITY PROCEDURES

1. General

A skilled and determined terrorist group can penetrate most office buildings. However, the presence and use of guards and physical security devices (e.g., exterior lights, locks, mirrors, visual devices) create a significant psychological deterrent. Terrorists are apt to shun risky targets for less protected ones. If terrorists decide to accept the risk, security measures can decrease their chance of success. Commanders should develop comprehensive building security programs and frequently conduct security surveys that provide the basis for an effective building security program. These surveys generate essential information for the proper evaluation of present security conditions and problems, available resources, and potential security policy. Being just one of the many facets in a complex structure, security policies must be integrated with other important areas such as fire safety, normal police procedures, work environment, and work transactions. The following information provides guidance when developing building security procedures.

2. Office Accessibility

a. Buildings most likely to be terrorist targets should not be directly accessible to the public.

b. Executive offices should not be located on the ground floor.

c. Locate senior personnel at the inner core of the building. This affords the best protection and control of visitors and prevents people outside the building from obtaining visual surveillance.

d. If building windows face public areas, reinforce them with bullet resistant materials and cover them with heavy curtains.

e. Monitor access to executive offices with a secretary, guard, or other individual who screens all persons and objects entering executive offices.

f. Place ingress door within view of the person responsible for screening personnel and objects passing through the door.

g. Doors may be remotely controlled by installing an electromagnetic door lock.

h. The most effective physical security configuration is to have doors locked from within and have only one visitor access door into the executive office area. Locked doors should have panic bars.

i. Depending upon the nature of the organization's activities, deception measures such as a large waiting area controlling access to several offices can be taken to draw attention away from the location and function of a particular office.

3. Physical Security Measures

a. Consider installing the following security devices: burglar alarm systems (preferably connected to a central security facility), sonic warning devices or other intrusion systems, exterior floodlights, dead bolt locks on doors, locks on windows, and iron grills or heavy screens for windows.

b. If feasible, add a 15- to 20-foot fence or wall and a comprehensive external lighting

system. External lighting is one of the cheapest and most effective deterrents to unlawful entry.

c. Position light fixtures where tampering would be difficult and noticeable.

d. Check grounds to ensure that there are no covered or concealed avenues of approach for terrorists and other intruders, especially near entrances.

e. Deny exterior access to fire escapes, stairways, and roofs.

f. Manhole covers near the building should be secured or locked.

g. Cover, lock, or screen outdoor openings (e.g., coal bins, air vents, utility access points).

h. Screen windows (particularly those near the ground or accessible from adjacent buildings).

i. Consider adding a thin, clear plastic sheet to windows to degrade the effects of flying glass in case of explosion.

j. Periodically inspect the interior of the entire building, including the basement and other infrequently used areas.

k. Locate outdoor trash containers, storage bins, and bicycle racks away from the building.

l. Book depositories or mail slots should not be adjacent to, or in, the building.

m. Mailboxes should not be close to the building.

n. Seal the top of voids and open spaces above cabinets, bookcases, and display cases.

o. Keep janitorial closets, service openings, telephone closets, and electrical closets locked at all times. Protect communications closets and utility areas with an alarm system.

p. Remove names and ranks on reserved parking spaces.

q. Empty trash receptacles daily (preferably twice a day).

r. Periodically check all fire extinguishers to ensure that they are in working order and readily available. Periodically check all smoke alarms to ensure that they are in working order.

4. Personnel Procedures

a. Stress heightened awareness by personnel working in the building, because effective building security depends largely on the actions and awareness of people.

b. Develop and disseminate clear instructions on personnel security procedures.

c. Hold regular security briefings for building occupants.

d. Personnel should understand security measures, appropriate responses, and should know who to contact in an emergency.

e. Conduct drills if appropriate.

f. Senior personnel should not work late on a routine basis. No one should ever work alone.

g. Give all personnel, particularly switchboard personnel and secretaries, special training in handling bomb threats and extortion telephone calls. Ensure that a bomb threat checklist and a pen or pencil are located at each telephone instrument.

h. Ensure the existence of secure communications systems between senior personnel, secretaries, and security personnel

with intercoms, telephones, and duress alarm systems.

i. Develop an alternate means of communications (e.g., two-way radio) in case the primary communications systems fail.

j. Do not open packages or large envelopes in buildings unless the sender or source is positively known. Notify security personnel of a suspicious package.

k. Have mail room personnel trained in bomb detection handling and inspection.

l. Lock all doors at night, on weekends, and when the building is unattended.

m. Maintain tight control of keys. Lock cabinets and closets when not in use.

n. When feasible, lock all building rest rooms when not in use.

o. Escort visitors in the building and maintain complete control of strangers who seek entrance.

p. Check janitors and their equipment before admitting them and observe while they are performing their functions.

q. Secure official papers from unauthorized viewing.

r. Update security clearances of employees (especially foreign nationals).

s. Do not reveal the location of building personnel to callers unless they are positively identified and have a need for the information.

t. Use extreme care when providing information over the telephone — remember, telephone lines may be tapped.

u. Do not give the names, positions, and especially home addresses or phone numbers of office personnel to strangers or telephone callers.

v. Do not list the address and telephone numbers of potential terrorist targets in books and rosters.

w. Avoid discussing travel plans or timetables in the presence of visitors.

x. Be alert to people disguised as public utility crews (e.g., road workers, vendors) who might station themselves near the building to observe activities and gather information.

y. Note parked or abandoned vehicles near the entrance to the building or near the walls.

z. Note the license plate number, make, model, year, and color of suspicious vehicles and the occupants' descriptions, and report that information to your supervisor, security officer, military and/or security police, or local police.

5. Controlling Entry

a. Consider installing a peephole, intercom, interview grill, or small aperture in entry doorways to screen visitors before the door is opened.

b. Use a reception room to handle visitors, thereby restricting their access to interior offices.

c. Consider installing metal detection devices at controlled entrances. Prohibit non-organization members from bringing boxes and parcels into the building.

d. Arrange building space so that unescorted visitors are under the receptionist's visual observation and to ensure that the visitors follow stringent access control procedures.

e. Do not make exceptions to the building's access control system.

f. Upgrade access control systems to provide better security through the use of intercoms, access control badges or cards, and closed circuit television.

6. Law Enforcement Procedures in the Area

a. Determine if the local or military law enforcement personnel patrol the area.

b. Request patrol by the local or military law enforcement personnel to include door checks after duty hours.

c. Know the capabilities and limitations of local and military law enforcement.

d. Use private guards if appropriate. Ensure that their background checks are completed before they assume duties.

e. Remember, the use of guards is a deterrent, not the primary source of security.

f. Brief and rehearse guards on appropriate responses in case of a terrorist incident.

7. Preparation for Emergencies

a. Maintain emergency items (e.g., supply of fresh water, nonperishable food, candles, lanterns, flashlights, extra batteries, blankets, portable radio, camping stove with spare fuel, axe, first aid kit, and other appropriate items).

b. Ensure that all members of the organization know the location of fire equipment, fire escapes, and other emergency exits as well as electrical service switches, weapons, and emergency radio.

c. Select and prepare an interior safe room for use in case of an attack.

- The safe room should have a sturdy door with a lock and an emergency exit if possible. Bathrooms on upper floors are good safe rooms.
- Store emergency and first aid supplies in the safe room. Bars or grillwork on safe room windows should be locked from the inside to expedite escape.
- Keep keys to locks, a rope or chain ladder to ease escape, and a means of communication (e.g., telephone or radio transmitter) in the safe room.

d. Select and identify emergency exits.

e. Determine evacuation and escape routes and brief personnel.

f. Senior personnel and secretaries should have duress switches that alarm at a constantly manned security office.

g. Maintain a set of written emergency and contingency procedures in the security office to assist rescue efforts.

h. Emergency procedures should include bomb threat and bomb search techniques.

8. Public Areas

a. Remove all potted plants and ornamental objects from public areas.

b. Empty trash receptacles frequently.

c. Lock doors to service areas.

d. Lock trapdoors in the ceiling or floor, including skylights.

e. Ensure that construction or placement of furniture and other items would not conceal explosive devices or weapons.

f. Keep furniture away from walls or corners.

g. Modify curtains, drapes, or cloth covers so that concealed items can be seen easily.

h. Box in the tops of high cabinets, shelves, or other fixtures.

i. Exercise particular precautions in public rest rooms.

j. Install springs on stall doors in rest rooms so they stand open when not locked. Equip stalls with an inside latch to prevent someone from hiding a device in a locked stall.

k. Install a fixed covering over the tops on commode water tanks.

l. Use open mesh baskets for soiled towels. Empty frequently.

m. Guards in public areas should have a way to silently alert the office of danger and to summon assistance (e.g., foot-activated buzzer).

Intentionally Blank

APPENDIX E
LOCK SECURITY

1. General

Locks or locking devices are the first line of defense in any security system. Locks are delaying devices of perimeter security and should be effectively integrated into other security and protection systems (e.g., alarms and electronic controls). There are five major categories of locks available for use in residences or offices: cylindrical, mortise, cylinder dead bolt, rim, and cylindrical lock sets with dead bolt functions. Residence, office, and vehicle security rely heavily upon locking devices that vary in appearance, function, and application.

2. Entryway Safety Factors

a. **Windows.** Windows pose more security problems than doors. Windows are available in a variety of styles and sizes and are often designed with little or no thought to security. The choice of window size or type is primarily based on ventilation, lighting, and esthetics. A window's only security value is that, if it is properly placed, it can make vulnerable areas unobservable. Intruders use windows to enter a building usually only as a last resort. They avoid breaking glass because of the noise made by its shattering and potential injury to themselves. The following techniques can be used to upgrade window security:

- For windows that slide up or down, the simplest measure is to drill one or more holes through the sash and frame and insert a pin or nail from the inside to prevent the window from being opened. Key-operated locks are also available, but they pose a safety hazard in the event the window is needed for escape in an emergency.
- Windows which don't open or are not intended for emergency exit should have steel bars, mesh, or grill work installed over them.

b. **Doors.** As important as the locking device is, the security afforded is only as good as the construction of the door and frame. There are four major types of doors: flush wood doors, turnstile, rail (panel) wood doors, and metal doors. There are two types of flush doors: hollow-core and solid-core. A hollow-core door is made of two sheets of thin veneer overlaying hollow cardboard strips. A solid-core door is made of two sheets of wood veneer overlapping a solid wooden core. Solid-core doors not only provide a substantial security advantage over hollow-core doors, they also add sound insulation and fire resistance. From a security perspective, a metal door is superior to any wooden door. A door's vulnerability (as opposed to its frame, hinges, or other accessory parts) is defined in terms of penetrability. (How easy is it to break through? How long does it take to break through?) However, breaking through a door is not the most common method of defeating a door system. A far more significant hazard is a door that fits loosely to the frame, thereby allowing it to be pried or forced open. Most wooden door frames have solid wood, 3/4-inch to 1-inch in depth. Beyond this, there is usually a 4-inch to 6-inch gap of air between the frame and the first stud. This construction provides very little resistance to forced entry. The following steps can be taken to enhance door security:

- **Strengthen the door frame.** Secure 2-inch x 4-inch studs directly behind the door frame's facing.

- **Install striker plates.** Striker plates vary in shape and are made for mortised or surface-mounted locks. A close fit between the lock and the striker plate reduces door movement when the door is closed. If the striker plate is not securely affixed to a sturdy door frame, it is easily forced apart.

- **Secure the door hinge.** The security value of the door hinge is often overlooked. A well-secured hinge prevents forcing a door out of its frame. From a security standpoint, the most important feature of a hinge is whether it is located on the inside or outside of the door. If the hinge pins are on the outside, they can be removed and the door removed from the frame. There are several solutions to this problem. One of the most effective methods is to weld the pins to the hinge. One method requires drilling a small hole through the hinge and into the pin, and then inserting a second pin or small nail flush with the hinge surface. Another method requires inserting two large screws in the door (or jamb) and leaving the screw head exposed 1/2-inch. Drill a matching hole on the opposite side so the screw head fits into the hole when the door is shut.

- **Secure sliding glass doors.** Sliding glass doors present easy access to a residence and pose complex security problems. These doors are available in a variety of styles and sizes and are designed with little or no thought to security. Many factors affect the ability to secure this type of entrance. It is not enough to prevent the door from being moved horizontally, it must also be secured vertically. The channel in which the door rides provide wide tolerances and facilitates vertically lifting the door out of its channel. Most locks designed for sliding glass doors take into consideration both types of movement and prevent the door from being lifted out of the channel. The simplest measure is to drill a hole through the channel and the frame. Insert a pin or nail to prevent the door from being opened and insert sheet metal screws into the upper channel, allowing them to protrude far enough to prevent the door from being lifted out of the channel.

c. **Locking Mechanisms**

- Cylindrical locks (key-in-knob locks) are the most widely used locks in residential construction. These locks are both inexpensive and simple to rekey. Cheap cylindrical locks have serious shortcomings. Cheaper cylindrical locks may not have a dead latch and may be slipped open with a credit card or celluloid strip. From a security point of view, these locks are the least desirable.

- Mortise locks fit into a cavity cut into the outer edge of the door. Since the introduction of cylindrical locks, the use of mortise locks has declined. Mortise locks are more expensive to install than cylindrical locks because large sections of the door and jamb have to be mortised to fit the lock. A quality mortise lock should have a dead bolt with enough throw to fit securely into the door frame.

- Rim locks are erroneously referred to as jimmy proof. Do not be misled by the use of the phrase "jimmy proof" because these locks can be compromised. However, rim locks are one of the most secure surface-mounted locks. Rim locks are not usually used as the primary lock. Install rim locks on the inside of the door above the vulnerable primary jamb. If a vertical dead bolt is used, the rim lock makes an excellent auxiliary lock and is very difficult to defeat.

- Cylindrical lock sets with dead bolt functions are comparative newcomers to the security hardware market. They combine the best features of a good security lock — a dead bolt function with a dead bolt lock. The better designs include a 1-inch throw dead bolt, a recessed cylinder to discourage forcible removal, a concealed armor plate to resist drilling, and a cylinder guard that spins freely when the dead bolt is in the locked position. The last feature makes it virtually impossible for an intruder to wrench the cylinder or cylinder guard off the door. These lock sets include a panic feature that ensures that the knob turns freely from the inside to permit rapid exit in case of emergency.

- Cylinder dead bolt locks are rapidly becoming the most popular auxiliary locks. They are installed above the primary lock. The best designs have steel bars and cylinder guards so they cannot be twisted, pried, or broken off. Double-cylinder locks may be a safety hazard where rapid escape is essential (e.g., in the case of fire) and are prohibited by many municipal codes in commercial facilities because fire officials are concerned that the need to find a key delays escape in an emergency.

d. **Lock Selection Guidelines**

- Consider locking hardware as a long-term investment that requires planning and exceptional quality.

- Match locks to the door and door frame to create a strong integral unit.

- Ensure that entrance door locks have a 1-inch dead bolt, a recessed cylinder to discourage forcible removal, and a cylinder guard that spins freely.

- Consider magnetic alarms if window or door glass is within arm's reach of a locking device.

- Consider alarm foil, resident alarm systems, and magnetic contacts if residence has large picture windows or sliding glass doors.

- Consider using padlocks to provide security protection to critical areas of the home. Padlocks should meet the following minimum requirements:

  •• A heavy shackle — at least 9/32-inch of hardened steel;

  •• A double-locking mechanism that locks the heel and toe;

  •• A minimum five-pin tumbler on tumbler locks; and

  •• A key-retaining feature that prevents removing the key unless the padlock is locked.

- Use rim locks to provide additional protection.

- Lock all vulnerable windows and doors at night.

- Ensure that entrance door hinges are heavy duty, pinned in the hinge, and equipped with door pins (metal pins or screws).

- Consider the possible safety hazards of using double-cylinder dead bolt locks that require key action on both sides.

- Check local fire safety codes before using double-cylinder dead bolt locks.

- Fill hollow metal door frames behind the striker plate with cement to prevent forcing the frame.
- Restrict access or distribution of home and office keys.
- Keep spare keys in a locked drawer or filing cabinet.
- Incorporate heavy-duty, double-cylinder door locks on office entrance doors if fire and safety regulations permit.

APPENDIX F
TELEPHONE CALL PROCEDURES

1. Upon receiving a threatening or suspicious telephone call:

a. Try to keep a verbatim record of the conversation.

b. Attempt to obtain the caller's name, address, and telephone number. Point out to the caller that by giving these details the caller is indicating that the call is a genuine warning.

c. Attempt to keep the caller talking and elicit further information if possible.

d. Summon assistance (through a telephone exchange) to trace the call and to corroborate facts and opinions.

e. Comply with the caller's request to be connected with another extension. Monitor the call if possible. Alert the officer of the day.

2. During the call:

a. Try to obtain answers to the questions listed on the telephone bomb threat checklist located in this appendix.

b. Try to determine the type of telephone call by contacting the operator immediately after the call ends. Was the call operator-connected? If the call was operator-connected, can the operator identify the source? Was it from a pay phone? If dialed from a pay phone, was it direct dialed?

3. After the call:

After the call is completed, provide the police duty officer with details of the telephone call and make a full written record of the conversation and any impressions, based on the information annotated on the telephone bomb threat checklist. This could be invaluable to the local or military police.

BUREAU OF ALCOHOL, TOBACCO AND FIREARMS (ATF)
BOMB THREAT CHECKLIST

Exact time of call _____
Exact words of caller _____

QUESTIONS TO ASK:

1. When will the bomb explode? _____
2. Where is the bomb? _____
3. What does the bomb look like? _____
4. What kind of bomb is it? _____
5. What will cause it to explode? _____
6. Did you place the bomb? _____
7. Why: _____
8. Where are you calling from? _____
9. What is your address? _____
10. What is your name? _____

CALLERS VOICE (circle)

Calm	Disguised	Nasal	Angry	Broken
Stutter	Slow	Sincere Lisp	Rapid	Giggling
Deep	Crying	Squeaky	Excited	Stressed
Accent Loud	Slurred	Normal		

If voice is familiar, whom did it sound like? _____
Were there any background noises? _____
Remarks: _____
_____
_____

Person receiving the call: _____
Telephone number call received at: _____
Date: _____

Report immediately to: _____
(refer to bomb incident plan)

APPENDIX G
CRISIS MANAGEMENT PLAN FORMAT

The format outlined on the following pages highlights areas of concern in crisis management planning. It is not meant to be all inclusive or rigidly followed. Note: This is a local format only and does not reflect a format developed and approved for use with operation plans or operation plans in concept format prepared by the combatant commanders to fulfill tasks assigned in the Joint Strategic Capabilities Plan, or as otherwise directed by the Chairman of the Joint Chiefs of Staff.

Copy No. ____ of ____ Copies
Issuing Headquarters _____
Location _____
Date-time-group_____

CRISIS MANAGEMENT PLAN

Refs: Maps, charts, and other relevant documents.

Time Zone: X

Task Organization: (List units organized to conduct antiterrorism operations. Include attachments, supporting roles, and delegation of authority as necessary.)

1. SITUATION (Identify essential information in order to understand ongoing events.)

a. **Terrorist Force** (Identify terrorist composition, disposition, methods of operation, estimated strength, and capabilities that could influence the crisis management operation. Refer to appropriate annex.)

b. **Response Forces** (Explain response force abilities and responsibilities. Response force ability can influence the crisis management mission.)

c. **Attachments and Detachments** (Address here or refer to an annex.)

d. **Assumptions** (Provide assumptions used as a basis for this plan [e.g., strength of response force to be supported, support available from other agencies]).

- **Tactical Situation Possibilities** (Obtained from the commander's planning guidance.)
- **Personnel Situation** (Provided by the personnel officer.)
- **Logistic Situation** (Provided by the logistics officer.)

- **Legal Situation Possibilities** (Provided by the staff judge advocate.)

- **Public Affairs Considerations** (Provided by PAO.)

2. MISSION (Identifies terrorism action mission. For example, "... to contain and neutralize terrorist threats and actions aimed at the disruption of this installation.")

3. EXECUTION

a. **Concept of Operations** (State commander's tactical plan. Purpose is to inform. May address how the commander will conduct combatting terrorism operations. Provides enough detail to insure proper action by subordinates in the absence of specific instructions. If the required details are extensive, address in an annex. If an operation involves two or more distinct phases, designate each phase and use subparagraphs [e.g., Phase I, Phase II]).

b. **Tasks** (Identify specific tasks for each element of the command charged with executing a crisis management mission. When giving multiple instructions, itemize and indicate priority or sequence [e.g., commander, reaction force]).

c. **Coordinating Instructions** (Include coordination and control measures applicable to two or more elements of the command.)

4. SERVICE SUPPORT (Provide a statement of service support instructions and arrangements supporting the crisis management operation. Use the following subparagraphs as required.)

a. **General** (Outline the general plan for service support.)

b. **Materiel and Services** (Address supply, transportation, labor [e.g., location of facilities, collection points, maintenance priority], and services [e.g., type of service available, designation and location of the unit, schedule of service] required.)

c. **Medical Evacuation and Hospitalization** (Provide the plan for evacuation and hospitalization of sick, wounded, or injured personnel. Address evacuation responsibilities and air evacuation policy.)

d. **Personnel** (Provide required information and instructions to supporting unit personnel.)

- **Maintenance of Unit Strength**

  •• **Strength Reports** (Provide instructions for submitting status reports. Include requirements for routine and special reports.)

  •• **Replacements** (Address validating existing personnel requisitions, instructions for submitting requisitions, and instructions for processing and removing replacements.)

- **Personnel Management** (Address military and civilian personnel and civilian detainee management procedures.)

- **Development and Maintenance of Morale**

  •• **Morale and Personnel Services** (Provide postal and finance services, religious activities, personal hygiene, and special services activity information.)

  •• **Mortuary Affairs** (Include evacuation procedures and handling of personal effects.)

- **Maintenance of Discipline, Law, and Order** (Provided by military law enforcement authority.)

- **Miscellaneous** (Include personnel administrative matters not specifically assigned to another coordinating staff section or included in preceding subparagraphs.)

e. **Miscellaneous** (Provide special instructions or special reports not covered in preceding paragraphs.)

5. COMMAND AND SIGNAL (Provide instructions for command and operation of communications-electronics equipment. Communications-electronics instructions may refer to an annex but should list the index and issue number of the command, control, communications, and computers operation instructions in effect. If not already issued, give instructions for control, coordination, and establishment of priorities in the use of electromagnetic emissions. Command instructions include subordinate and higher unit command post locations and designated alternate command posts.)

6. ACKNOWLEDGE INSTRUCTIONS

/s/
Commander

Annexes as applicable

Distribution:

Intentionally Blank

APPENDIX H
CRISIS MANAGEMENT PLAN CHECKLIST

General. Unit antiterrorism success will depend on the degree and seriousness of the crisis management planning. The following checklist identifies items for use by joint force commanders and component commander staffs in analyzing antiterrorism plans within their commands.

YES NO

1. Intelligence and/or Counterintelligence

___ ___ Does the plan allow for the threat analysis process (e.g., collection, analysis, production, and dissemination) to aid in the identification of the local threat?

___ ___ Does the plan consider restrictions placed on the collection and storage of information?

___ ___ Does the plan indicate an awareness of sources of information for the threat analysis process (e.g., military intelligence, counterintelligence, Federal agencies, and state and local authorities)?

___ ___ Does the plan allow for liaison and coordination of information (e.g., establishing a threat analysis committee)?

2. Threat Assessment

___ ___ Does the plan identify the local threat (immediate and long term)?

___ ___ Does the plan identify other threats (e.g., national and international groups that have targeted or might target US installations)?

___ ___ Does the installation incorporate factors of the assessing the threat? Does it address:

___ ___ Geography of the area concerned;

___ ___ Law enforcement resources;

___ ___ Population cultural factors; and

___ ___ Communications capabilities?

___ ___ Does the plan establish a priority of identified weaknesses and vulnerabilities?

___ ___ Is the threat assessment periodically updated?

3. Security Countermeasures

___ ___ Does the plan have specified THREATCONs and recommended actions?

___ ___ Do security countermeasures include a combination of physical operations and sound-blanketing security measures?

___ ___ Do the THREATCONs correspond to Appendix BB of DODD O-2000.12H, "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence"?

4. OPSEC

___ ___ Have procedures been established that prevent terrorists from readily obtaining information about plans and operations (e.g., not publishing the commanding general's itinerary, safeguarding classified material)?

___ ___ Does the plan allow for in-depth coordination with the installations OPSEC program?

___ ___ Has an OPSEC annex been included in the contingency plan?

5. Personnel Security

___ ___ Has the threat analysis identified individuals vulnerable to terrorist attack?

___ ___ Has a training program been established to educate both military and civilian personnel in the proper techniques of personnel protection and security commensurate with the local threat and the type of position held?

6. Physical Security

___ ___ Are special threat plans and physical security plans mutually supportive?

___ ___ Do security measures establish obstacles to terrorist activity (e.g., guards, host-nation forces, lighting, fencing)?

___ ___ Does the special threat plan include the threats identified in the threat statements of higher headquarters?

___ ___ Does the physical security officer assist in the threat analysis and corrective action?

___ ___ Is there obvious command interest in physical security?

___ ___ Does the installation have and maintain detection systems and an appropriate assessment capability?

7. Security Structure

___ ___ Does the plan indicate that the FBI has primary domestic investigative and operational responsibility in the United States and US territories?

___ ___ Has coordination with the staff judge advocate been established?

___ ___ Does the plan allow for close cooperation between principal agents of the military, civilian, and host-nation communities and Federal agencies?

___ ___ Does the plan clearly indicate parameters for use of force, including the briefing of any elements augmenting military police assets?

___ ___ Is there a mutual understanding between all local agencies (e.g. military, local FBI resident or senior agent-in-charge, host-nation forces and local law enforcement) that might be involved in a terrorist incident on the installation regarding authority, jurisdiction, and possible interaction?

___ ___ Has the staff judge advocate considered ramifications of closing the post (e.g., possible civilian union problems)?

___ ___ Does the plan identify the DOS as having primary investigative and operational responsibility overseas?

8. Operations Center Training

___ ___ Has the operational command and coordination center (operations center) been established and exercised?

___ ___ Is the operational command and coordination center based on the needs of the installation while recognizing manpower limitations, resource availability, equipment, and command?

___ ___ Does the plan include a location for the operations center?

___ ___ Does the plan designate alternate locations for the operations center?

___ ___ Does the plan allow for the use of visual aids (chalkboards, maps with overlays, bulletin boards) to provide situation status reports and countermeasures?

___ ___ Does the plan create and designate a location for a media center?

___ ___ Have the operations and media centers been activated together within the last quarter?

___ ___ Does the operations center have SOPs covering communications and reports to higher headquarters?

___ ___ Does the operations center offer protection from terrorist attack?

9. Reaction Force Training

___ ___ Has the force been trained and exercised under realistic conditions?

___ ___ Has corrective action been applied to shortcomings and deficiencies?

___ ___ Has the reaction force been formed and mission-specified trained (e.g., building entry and search techniques, vehicle assault operations, countersniper techniques, equipment)?

___ ___ Has the reaction force been tested quarterly (alert procedures, response time, overall preparedness)?

___ ___ Has responsibility been fixed for the negotiation team? Has the negotiation team been trained and exercised under realistic conditions?

___ ___ Does the negotiation team have the proper equipment?

10. General Observations

___ ___ Was the plan developed as a coordinated staff effort?

___ ___ Does the plan outline reporting requirements (e.g., logs, journals, after-action report)?

___ ___ Does the plan address presence of the media?

___ ___ Does the plan include communications procedures and communications nets?

___ ___ Does the plan consider the possible need for interpreters?

___ ___ Does the plan consider the need for a list of personnel with various backgrounds to provide cultural profiles on foreign subjects and victims, as well as to assist with any negotiation efforts?

___ ___ Does the plan provide for and identify units that will augment military police assets?

___ ___ Does the plan delineate specific tasking(s) for each member of the operations center?

___ ___ Does the plan provide for a response for each phase of antiterrorism activity (e.g., initial response, negotiation, assault)?

___ ___ Does the plan designate service support communications?

___ ___ Does the plan make provisions for notification of accident and incident control officer?

___ ___ Does the plan provide for EOD support?

___ ___ Does the plan take into consideration the movement from various locations, including commercial airports, of civilian and military advisory personnel with military transportation assets?

___ ___ Does the plan allow for the purchase and/or use of civilian vehicles, supplies, food, if needed (including use to satisfy a hostage demand)? Does the plan make provisions for paying civilian employees overtime if they are involved in a special threat situation?

___ ___ Does the plan take into consideration the messing, billeting, and transportation of civilian personnel?

___ ___ Do appropriate personnel have necessary language training?

___ ___ Is MWD support available?

Intentionally Blank

APPENDIX J
THREATCON SYSTEM

SECTION I. BASIC THREATCON PROCEDURES

1. General

The THREATCONs outlined below describe the progressive level of a terrorist threat to all US military facilities and personnel under DODD 2000.12, "DoD Combating Terrorism Program." As approved by the Chairman of the Joint Chiefs of Staff, the terminology and definitions are recommended security measures designed to ease inter-Service coordination and support of US military AT activities. The purpose of the THREATCON system is to provide accessibility to, and easy dissemination of, appropriate information. The declaration, reduction, and cancellation of THREATCONs remain the exclusive responsibility of commanders. Although there is no direct correlation between threat information (e.g., intelligence summaries, warning reports, and spot reports) and THREATCONs, such information, coupled with the guidance provided below, assists commanders in making prudent THREATCON declarations. THREATCONs may also be suffixed with the geographic area deemed at risk. Once a THREATCON is declared, the selected security measures are implemented immediately. NOTE: When used in AT plans, recommend that the information contained in this appendix be marked "For Official Use Only" in accordance with DOD Regulation 5400.7-R. The DODD 2000.12, "DoD Combating Terrorism Program," recommended measures are as follows:

a. **THREATCON NORMAL** exists when a general threat of possible terrorist activity exists but warrants only a routine security posture.

b. **THREATCON ALPHA** applies when there is a general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of THREATCON BRAVO measures. However, it may be necessary to implement certain measures from higher THREATCONs either resulting from intelligence received or as a deterrent. The measures in this THREATCON must be capable of being maintained indefinitely.

- **Measure 1.** At regular intervals, remind all personnel and dependents to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers. Watch for unidentified vehicles on or in the vicinity of US installations. Watch for abandoned parcels or suitcases and any unusual activity.

- **Measure 2.** The duty officer or personnel with access to building plans as well as the plans for area evacuations must be available at all times. Key personnel should be able to seal off an area immediately. Key personnel required to implement security plans should be on-call and readily available.

- **Measure 3.** Secure buildings, rooms, and storage areas not in regular use.

- **Measure 4.** Increase security spot checks of vehicles and persons entering the installation and unclassified areas under the jurisdiction of the United States.

- **Measure 5.** Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.

- **Measure 6.** As a deterrent, apply measures 14, 15, 17, or 18 from THREATCON BRAVO, either individually or in combination with each other.

- **Measure 7.** Review all plans, orders, personnel details, and logistic requirements related to the introduction of higher THREATCONs.

- **Measure 8.** Review and implement security measures for high-risk personnel as appropriate.

- **Measure 9.** As appropriate, consult local authorities on the threat and mutual antiterrorism measures.

- **Measure 10.** To be determined.

c. **THREATCON BRAVO** applies when an increased and more predictable threat of terrorist activity exists. The measures in this THREATCON must be capable of being maintained for weeks without causing undue hardship, affecting operational capability, and aggravating relations with local authorities.

- **Measure 11.** Repeat measure 1 and warn personnel of any other potential form of terrorist attack.

- **Measure 12.** Keep all personnel involved in implementing antiterrorist contingency plans on call.

- **Measure 13.** Check plans for implementation of the next THREATCON.

- **Measure 14.** Move cars and objects (e.g., crates, trash containers) at least 25 meters from buildings, particularly buildings of a sensitive or prestigious nature. Consider centralized parking.

- **Measure 15.** Secure and regularly inspect all buildings, rooms, and storage areas not in regular use.

- **Measure 16.** At the beginning and end of each workday, as well as at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious packages.

- **Measure 17.** Examine mail (above the regular examination process) for letter or parcel bombs.

- **Measure 18.** Check all deliveries to such locations as messes and clubs. Advise dependents to check home deliveries.

- **Measure 19.** Increase surveillance of domestic accommodations, schools, messes, clubs, and other soft targets to improve deterrence and defense and to build confidence among staff and dependents.

- **Measure 20.** Make staff and dependents aware of the general situation in order to stop rumors and prevent unnecessary alarm.

- **Measure 21.** At an early stage, inform members of local security committees of actions being taken. Explain reasons for actions.

- **Measure 22.** Physically inspect visitors and randomly inspect their suitcases, parcels, and other containers. Identify the visitor's destination. Ensure that proper dignity is maintained and, if possible, ensure that female visitors are inspected only by a female qualified to conduct physical inspections.

- **Measure 23.** Operate random patrols to check vehicles, people, and buildings.

- **Measure 24.** Protect off-base military personnel and military vehicles in accordance with prepared plans. Remind drivers to lock vehicles and check vehicles before entering or exiting the vehicle.

- **Measure 25.** Implement additional security measures for high-risk personnel as appropriate.

- **Measure 26.** Brief personnel who may augment guard forces on the use of deadly force. Ensure that there is no misunderstanding of these instructions.

- **Measures 27.** As appropriate, consult local authorities on the threat and mutual antiterrorism measures.

- **Measures 28 and 29.** To be determined.

d. **THREATCON CHARLIE** applies when an incident occurs or intelligence is received indicating that some form of terrorist action against personnel and facilities is imminent. Implementation of measures in this THREATCON for more than a short period probably will create hardship and affect the peacetime activities of the unit and its personnel.

- **Measure 30.** Continue, or introduce, all measures listed in THREATCON BRAVO.

- **Measure 31.** Keep all personnel responsible for implementing antiterrorist plans at their places of duty.

- **Measure 32.** Limit access points to the absolute minimum.

- **Measure 33.** Strictly enforce control of entry. Randomly search vehicles.

- **Measure 34.** Enforce centralized parking of vehicles away from sensitive buildings.

- **Measure 35.** Issue weapons to guards. Local orders should include specific orders on issue of ammunition.

- **Measure 36.** Increase patrolling of the installation.

- **Measure 37.** Protect all designated vulnerable points. Give special attention to vulnerable points outside the military establishment.

- **Measure 38.** Erect barriers and obstacles to control traffic flow.

- **Measure 39.** Consult local authorities about closing public (and military) roads and facilities that might make sites more vulnerable to attacks.

- **Measure 40.** To be determined.

e. **THREATCON DELTA** applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is likely. Normally, this THREATCON is declared as a localized condition.

- **Measure 41.** Continue, or introduce, all measures listed for THREATCONs ALPHA, BRAVO, and CHARLIE.

- **Measure 42.** Augment guards as necessary.

- **Measure 43.** Identify all vehicles within operational or mission-support areas.

- **Measure 44.** Search all vehicles and their contents before allowing entrance to the installation.

- **Measure 45.** Control access and implement positive identification of all personnel — no exceptions.

- **Measure 46.** Search all suitcases, briefcases, and packages brought into the installation.

- **Measure 47.** Control access to all areas under the jurisdiction of the United States.
- **Measure 48.** Make frequent checks of the exterior of buildings and of parking areas.
- **Measure 49.** Minimize all administrative journeys and visits.
- **Measure 50.** Coordinate the possible closing of public and military roads and facilities with local authorities.
- **Measure 51.** To be determined.

SECTION II. SHIPBOARD TERRORIST THREAT CONDITIONS

2. Shipboard Terrorist THREATCON Measures

The measures outlined below are for use aboard vessels and serve two purposes. First, the crew is alerted, additional watches are created, and there is greater security. Second, these measures display the ship's resolve to prepare for and counter the terrorist threat. These actions will convey to anyone observing the ship's activities that the ship is prepared, the ship is an undesirable target, and the terrorist(s) should look elsewhere for a vulnerable target. The measures outlined below do not account for local conditions and regulations or current threat intelligence. The ship's command must maintain flexibility. As threat conditions change, the ship's crew must be prepared to take actions to counter the threat. When necessary, additional measures must be taken immediately. The simple solution to THREATCON CHARLIE or DELTA is to get under way, but this option may not always be available.

a. **THREATCON ALPHA** is declared when a general threat of possible terrorist activity is directed toward installations, vessels, and personnel, the nature and extent of which are unpredictable and where circumstances do not justify full implementation of THREATCON BRAVO measures. However, it may be necessary to implement certain selected measures from THREATCON BRAVO as a result of intelligence received or as a deterrent. The measures in this threat condition must be capable of being maintained indefinitely.

- **Measure 1.** Brief crew on the threat, ship security, and security precautions to be taken while ashore.
- **Measure 2.** Muster and brief security personnel on the threat and ROE.
- **Measure 3.** Review security plans and keep them available. Keep on call key personnel who may be needed to implement security measures.
- **Measure 4.** Consistent with local rules, regulations, and SOFAs, post qualified armed fantail sentry and forecastle sentry. Rifles are the preferred weapon.
- **Measure 5.** Consistent with local rules, regulations, and SOFAs, post qualified armed pier sentry and pier entrance sentry.
- **Measure 6.** Issue two-way radios to all sentries, roving patrols, quarterdeck watch, and response force. If practical, all guards will be equipped with at least two systems of communication (e.g., two-way radio, telephone, whistle, or signal light).
- **Measure 7.** Issue night vision devices to selected posted security personnel.

- **Measure 8.** Coordinate pier and fleet landing security with collocated forces and local authorities. Identify anticipated needs for mutual support (security personnel, boats, and equipment) and define methods of activation and communication.

- **Measure 9.** Tighten shipboard and pier access control procedures. Positively identify all personnel entering pier and fleet landing area — no exceptions.

- **Measure 10.** Consistent with local rules, regulations, and SOFAs, establish unloading zone(s) on the pier away from the ship.

- **Measure 11.** Deploy barriers to keep vehicles away from the ship. Barriers may be ship's vehicles, equipment, or items available locally.

- **Measure 12.** Post signs in local language(s) to explain visiting and loitering restrictions.

- **Measure 13.** Inspect all vehicles entering pier and check for unauthorized personnel, weapons, and/or explosives.

- **Measure 14.** Inspect all personnel, hand-carried items, and packages before they come aboard. Where possible, screening should be at the pier entrance or foot of brow.

- **Measure 15.** Direct departing and arriving liberty boats to make a security tour around the ship and give special attention to the waterline and hull. Boats must be identifiable night and day to ship's personnel.

- **Measure 16.** Water taxis, ferries, bum boats, and other harbor craft require special concern because they can serve as an ideal platform for terrorists. Unauthorized craft should be kept away from the ship; authorized craft should be carefully controlled, surveilled, and covered.

- **Measure 17.** Identify and inspect work boats.

- **Measure 18.** Secure spaces not in use.

- **Measure 19.** Regulate shipboard lighting to best meet the threat environment. Lighting should include illumination of the waterline.

- **Measure 20.** Rig hawsepipe covers and rat guards on all lines, cable, and hoses. Consider using an anchor collar.

- **Measure 21.** Raise accommodation ladders, stern gates, and jacob ladders when not in use. Clear ship of all unnecessary stages, camels, barges, oil donuts, and lines.

- **Measure 22.** Conduct security drills to include bomb threat and repel boarders exercises.

- **Measure 23.** Review individual actions in THREATCON BRAVO for possible implementation.

- **Measure 24.** To be determined.

b. **THREATCON BRAVO** is declared when an increased and more predictable threat of terrorist activity exists. The measures in this THREATCON must be capable of being maintained for weeks without causing undue hardships, without affecting operational capability, and without aggravating relations with local authorities.

- **Measure 25.** Maintain appropriate THREATCON ALPHA measures.

- **Measure 26.** Review liberty policy in light of the threat and revise it as necessary to maintain the safety and security of the ship and crew.

- **Measure 27.** Conduct divisional quarters at foul weather parade to determine the status of on-board personnel and to disseminate information.

- **Measure 28.** Ensure that an up-to-date list of bilingual personnel for the operational area is readily available. Ensure that the warning tape in the pilot house and/or quarterdeck that warns small craft to remain clear is in both the local language and English.

- **Measure 29.** Remind all personnel to: (a) be suspicious and inquisitive of strangers, particularly those carrying suitcases or other containers; (b) be alert for abandoned parcels or suitcases; (c) be alert for unattended vehicles in the vicinity; (d) be wary of any unusual activities; and (e) notify the duty officer of anything suspicious.

- **Measure 30.** Remind personnel to lock their parked vehicles and to carefully check them before entering.

- **Measure 31.** Designate and brief picket boat crews. Prepare boats and place crews on 15-minute alert. If the situation warrants, make random picket boat patrols in the immediate vicinity of the ship with the motor whaleboat or gig. Boat crews will be armed with M16 rifles, one M60 with 200 rounds of ammunition, and 10 concussion grenades.

- **Measure 32.** Consistent with local rules, regulations, and SOFAs, establish armed brow watch on pier to check identification and inspect baggage before personnel board ship.

- **Measure 33.** Man signal bridge or pilot house and ensure that flares are available to ward off approaching craft.

- **Measure 34.** After working hours, place armed sentries on a superstructure level from which they can best cover areas about the ship.

- **Measure 35.** Arm all members of the quarterdeck watch and SAT. In the absence of a SAT, arm two members of the self defense force (SDF).

- **Measure 36.** Provide shotgun and ammunition to quarterdeck. If the situation warrants, place sentry with shotgun inside the superstructure at a site from which the quarterdeck can be covered.

- **Measure 37.** Issue arms to selected qualified officers to include command duty officer and assistant command duty officer.

- **Measure 38.** Arm sounding and security patrol.

- **Measure 39.** Muster and brief ammunition bearers or messengers.

- **Measure 40.** Implement procedures for expedient issue of firearms and ammunition from small arms locker (SAL). Ensure that a set of SAL keys are readily available and in the possession of an officer designated for this duty by the commanding officer.

- **Measure 41.** Load additional small arms magazines to ensure adequate supply for security personnel and response forces.

- **Measure 42.** Inform local authorities of actions taken as the THREATCON increases.
- **Measure 43.** Test communications with local authorities and other US Navy ships in port.
- **Measure 44.** Instruct watches to conduct frequent random searches under piers, with emphasis on potential hiding places, pier pilings, and floating debris.
- **Measure 45.** Conduct searches of the ship's hull and boats at intermittent intervals and immediately before it puts to sea.
- **Measure 46.** Move cars and objects such as crates and trash containers 100 feet from the ship.
- **Measure 47.** Hoist boats aboard when not in use.
- **Measure 48.** Terminate all public visits.
- **Measure 49.** Set materiel condition YOKE, main deck and below.
- **Measure 50.** After working hours, reduce entry points to the ship's interior by securing selected entrances from the inside.
- **Measure 51.** Duty department heads ensure that all spaces not in regular use are secured and inspected periodically.
- **Measure 52.** If two brows are rigged, remove one of them.
- **Measure 53.** Maintain capability to get under way on short notice or as specified by SOPs. Consider possible relocation sites (such as a different pier or anchorage). Rig brow and accommodation ladder for immediate raising or removal.
- **Measure 54.** Ensure that .50-caliber mount assemblies are in place with ammunition in ready service lockers (.50-caliber machine guns will be maintained in the armory, pre-fire checks completed, and ready for use).
- **Measure 55.** Prepare fire hoses. Brief designated personnel on procedures for repelling boarders, small boats, and ultra-light aircraft.
- **Measure 56.** Obstruct possible helicopter landing areas in such a manner as to prevent hostile helicopters from landing.
- **Measure 57.** Review riot and crowd control procedures, asylum-seeker procedures, and bomb threat procedures.
- **Measure 58.** Monitor local communications (e.g., ship-to-ship, TV, radio, police scanners).
- **Measure 59.** Implement additional security measures for high-risk personnel as appropriate.
- **Measure 60.** Review individual actions in THREATCON CHARLIE for possible implementation.
- **Measures 61 and 62.** To be determined.

c. **THREATCON CHARLIE** is declared when an incident occurs or intelligence is received indicating that some form of terrorist action against installations, vessels, or personnel is imminent. Implementation of this THREATCON for more than a short period will probably create hardship and will affect the peacetime activities of the ship and its personnel.

- **Measure 63.** Maintain appropriate measures for THREATCONs ALPHA and BRAVO.

- **Measure 64.** Cancel liberty. Execute emergency recall.
- **Measure 65.** Be prepared to get under way on one (1) hour's notice or less. If conditions warrant, request permission to sortie.
- **Measure 66.** Muster and arm SAT, BAF, and RF. Position SAT and BAF at designated location(s). Deploy RF to protect command structure and augment posted security watches.
- **Measure 67.** Place armed sentries on a superstructure level from which they can best cover areas about the ship.
- **Measure 68.** Establish .50- or .30-caliber machine gun positions.
- **Measure 69.** If available, deploy STINGER surface-to-air missiles in accordance with established ROE.
- **Measure 70.** Energize radar and establish watch.
- **Measure 71.** Ships with high-power sonars operate actively for random periods to deter underwater activity. Man passive sonar capable of detecting boats, swimmers, or underwater vehicles. Position any non-sonar-equipped ships within the acoustic envelope of sonar-equipped ships.
- **Measure 72.** Man one or more repair lockers. Establish communications with an extra watch in damage control central.
- **Measure 73.** Deploy picket boat. Boats should be identifiable night and day from the ship (e.g., by lights or flags).
- **Measure 74.** If feasible, deploy a helicopter as an observation or gun platform. The helicopter should be identifiable night and day from the ship.
- **Measure 75.** Activate antiswimmer watch. (Portions of watch may already be implemented by previous THREATCON measures).
- **Measure 76.** Issue weapons to selected officers and chief petty officers in the duty section (i.e., the commanding officer, executive officer, department heads).
- **Measure 77.** Issue concussion grenades to topside rovers, forecastle and fantail sentries, and bridge watch.
- **Measure 78.** Erect barriers and obstacles as required to control traffic flow.
- **Measure 79.** Strictly enforce entry control procedures and searches — no exceptions.
- **Measure 80.** Enforce boat exclusion zone.
- **Measure 81.** Minimize all off-ship administrative trips.
- **Measure 82.** Discontinue contract work.
- **Measure 83.** Set materiel condition ZEBRA, second deck and below.
- **Measure 84.** Secure from the inside all unguarded entry points to the interior of the ship.
- **Measure 85.** Rotate screws and cycle rudder(s) at frequent and irregular intervals.
- **Measure 86.** Rig additional firehoses. Charge the firehoses when manned just prior to actual use.

- **Measure 87.** Review individual actions in THREATCON DELTA for implementation.

- **Measure 88.** To be determined.

d. **THREATCON DELTA** is declared when a terrorist attack has occurred in the immediate area or intelligence has been received that indicates a terrorist action against a specific location or person is likely. Normally, this THREATCON is declared as a localized warning.

- **Measure 89.** Maintain appropriate THREATCONs ALPHA, BRAVO, and CHARLIE measures.

- **Measure 90.** Permit only necessary personnel topside.

- **Measure 91.** Prepare to get under way and, if possible, cancel port visit and depart.

- **Measure 92.** Post sentries with fully automatic weapons to cover possible helicopter landing areas.

- **Measure 93.** Arm selected personnel of the SDF.

- **Measure 94.** Deploy grenade launchers to cover approaches to ship.

- **Measure 95.** To be determined.

SECTION III. AVIATION FACILITY THREATCON PROCEDURES

3. General

In addition to basic THREATCON procedures, a variety of other tasks may need to be performed at aviation facilities. This is particularly true for airbases located in areas where the threat of terrorist attacks is high.

a. **THREATCONs ALPHA AND BRAVO**

- **Planning**

  •• Review THREATCONs ALPHA and BRAVO measures.

  •• Update THREATCONs ALPHA and BRAVO measures as required.

- **Briefing and Liaison**

  •• Brief all personnel on the threat, especially pilots, ground support crews, and air traffic controllers.

  •• Inform local police of the threat. Coordinate plans to safeguard aircraft flight paths into and out of air stations.

  •• Ensure that duty officers are always available by telephone.

  •• Prepare to activate contingency plans and issue detailed air traffic control procedures if appropriate.

  •• Be prepared to receive and direct aircraft from other stations.

- **Precautions Inside the Perimeter**

  •• Perform thorough and regular inspection of areas within the perimeters from which attacks on aircraft can be made.

  •• Take action to ensure that no extremists armed with surface-to-air missiles can operate against aircraft within the perimeter.

  •• Establish checkpoints at all entrances and inspect all passes and permits.

Identify documents of individuals entering the area — no exceptions.

•• Search all vehicles, briefcases, and packages entering the area.

•• Erect barriers around potential targets if at all possible.

•• Maintain firefighting equipment and conduct practice drills.

•• Hold practice alerts within the perimeter.

- **Precautions Outside the Perimeter**

•• Conduct, with local police, regular inspections of the perimeter — especially the area adjacent to flight paths.

•• Advise the local police of any areas outside the perimeter where attacks could be mounted and that cannot be avoided by aircraft on takeoff or landing.

•• Advise aircrews to report any unusual activity near approach and overshoot areas.

b. **THREATCON CHARLIE**

- **Planning**

•• Review THREATCON CHARLIE measures.

•• Update THREATCON CHARLIE measures as required.

- **Briefing and Liaison**

•• Brief all personnel on the increased threat.

•• Inform local police of increased threat.

•• Coordinate with the local police on any precautionary measures taken outside the airfield's perimeters.

•• Implement appropriate flying countermeasures specified in SOPs when directed by air traffic controllers.

- **Precautions Inside the Perimeter**

•• Inspect all vehicles and buildings on a regular basis.

•• Detail additional guards to be on call at short notice and consider augmenting firefighting details.

•• Carry out random patrols within the airfield perimeter and maintain continuous observation of approach and overshoot areas.

•• Reduce flying to essential operational flights only. Cease circuit flying if appropriate.

•• Escort all visitors.

•• Close relief landing grounds where appropriate.

•• Check airfield diversion state.

- **Precautions Outside the Perimeter**

•• Be prepared to react to requests for assistance.

•• Provide troops to assist local police in searching for terrorists on approaches outside the perimeter of military airfields.

c. **THREATCON DELTA**

- **Planning**

•• Review THREATCON DELTA measures.

•• Update THREATCON DELTA measures as required.

- **Briefings and Liaison**

•• Brief all personnel on the very high levels of threat.

•• Inform local police of the increased threat.

- **Precautions Inside the Perimeter**

•• Cease all flying except for specifically authorized operational sorties.

•• Implement, if necessary, appropriate flying countermeasures.

•• Be prepared to accept aircraft diverted from other stations.

•• Be prepared to deploy light aircraft and helicopters for surveillance tasks or to move internal security forces.

- **Precautions Outside the Perimeter**

•• Close military roads allowing access to the airbase.

Intentionally Blank

APPENDIX K
EXPLOSIVE DEVICE PROCEDURES

1. Search and Evacuation Procedures for a Suspected IED

a. Suspicion that an IED is within an establishment often stems from a threatening anonymous telephone call. Treat the call seriously even though subsequent investigation may prove it to be a false alarm or hoax. Appendix F, "Telephone Call Procedures," provides advice on handling anonymous telephone calls.

b. Upon receiving an anonymous warning or threat, notify the military law enforcement authorities or police immediately. Local SOPs determine subsequent actions. Immediate action may include search without evacuation, movement of personnel within the establishment, partial evacuation, or total evacuation.

- Factors favoring a search before movement of personnel include the following:

  •• There is a high incidence of hoax telephone threats.

  •• Effective security arrangements have been established.

  •• Information in the warning is imprecise or incorrect.

  •• The caller sounded intoxicated, amused, or very young.

  •• The prevailing threat of terrorist activity is low.

  •• Physical security in place (checks of all incoming packages, visitor escort) would prevent the placement of a bomb.

- Factors favoring movement of personnel before searching include the following:

  •• The area (e.g., post or base) is comparatively open.

  •• Information in the warning is precise as to matters of location, description of device, timing, and motive for attack.

  •• Prevailing threat of terrorist activity is high.

  •• A suspicious package or bomb-looking devices are discovered.

c. **Searching for a Suspected IED**

- Use a nominated persons search when the threat's credibility is very low. Predesignated individuals search assigned areas. The search can be completed in a short time or can be done covertly.

- Use an occupant search when the threat's credibility is low. Occupants search their own areas. The search is completed quickly because occupants know their area and are most likely to notice anything unusual.

- Use a team search when the threat's credibility is high. Search teams make a systematic search of the area. The search is slow and thorough, and places the minimum number of personnel at risk. Completely evacuate the area and ensure that it remains evacuated until the search is complete.

- Use patrol-explosive MWD, if available, as a final means of checking the situation in each instance.

d. **Search Procedures**

- Make an audio check and listen for unusual sounds.
- Visually sweep the area up to the waist, then sweep up to the ceiling. Do not forget the tops of cabinets and cupboards.
- Perform a thorough and systematic search in and around containers and fixtures.
- Pass search results as quickly as possible to the leader responsible for controlling the search area.

e. **Search Organization.** Search parties are designated by the commander or senior DOD civilian in charge of the site. The person controlling the search should possess a means of tracking and recording the search results (e.g., a diagram of the area). Delegate areas of responsibility to search team leaders who report to the person controlling the search when their areas have been cleared. Pay particular attention to entrances, toilets, corridors, stairs, unlocked closets, storage spaces, rooms, and areas not checked by usual occupants—external building areas, window ledges, ventilators, courtyards, and spaces shielded from normal view. Searchers must be familiar with the area so that they can readily identify unusual or foreign objects.

f. **Evacuation Procedures.** Evacuation procedures depend upon circumstances. Prepare, publicize, and rehearse evacuation plans in advance. Address alarm systems, assembly areas, routes to assembly areas, personnel evacuation response, building and area clearance, and evacuation drills.

g. **Alarm System.** The bomb threat alarm system should be easily distinguished from the fire alarm.

h. **Assembly Areas.** Assembly areas are preselected and well known to personnel. Establish a clearly defined procedure for controlling, marshalling, and checking personnel within the assembly area. If buildings or establishments are in a public area, coordinate assembly areas with local police. Assembly areas are chosen with the following considerations:

- Assembly areas should be at least 200 meters and not less than 100 meters from the likely target or building, if at all possible.
- Locate assembly areas where there is little chance of an IED being hidden. Open spaces are best. Avoid car parking areas — IEDs can be easily hidden in vehicles.
- Select alternate assembly areas to reduce the likelihood of ambush with a second device or small arms fire. If possible, search the assembly area before personnel occupy the space.
- Assembly areas should not be near expanses of plate glass or windows. Blast effects can cause windows to be sucked outward rather than blown inward.

i. **Routes to Assembly Areas.** Choose routes to the assembly area so that personnel do not approach the IED at any time. Preselect routes to the assembly area, but devise a system to inform personnel of the location of the suspected IED and alternate routes. Routes prevent confusion and bunching and avoid potential hazards (e.g., plate glass, windows, and likely locations of additional IEDs).

j. **Personnel Evacuation Response.** Upon hearing the alarm, personnel secure all classified documents, conduct a quick visual search of their immediate working area, open

windows wherever possible, leave the building taking only valuable personal belongings, leave doors open, and immediately proceed to the assembly area.

k. **Building and Area Clearance.** Establish procedures to ensure that threatened buildings and areas are cleared and to prevent people from reentering the building. Establish a cordon to prevent personnel from entering the danger area. Establish an incident control point (ICP) as the focal point for military law enforcement and police control.

l. **Evacuation Drills.** Periodically practice evacuation and search drills under the supervision of the installation or unit senior officer. Hold drills in cooperation with local police if possible. Avoid unnecessarily alarming personnel and civilians in adjacent premises.

2. Discovery of a Suspected IED

Do not touch or move a suspicious object. If it is possible for someone to account for the presence of the object, then ask the person to identify it with a verbal description. This should not be done if it entails bringing evacuated personnel back into the area. Take the following actions if an object's presence remains inexplicable:

a. Evacuate buildings and surrounding areas, including the search team.

b. Evacuated areas must be at least 100 meters from the suspicious object.

c. Establish a cordon and ICP.

d. Inform the ICP that an object has been found.

e. Keep person who located the object at the ICP until questioned.

f. Cordon suspicious objects to a distance of at least 100 meters and cordon suspicious vehicles to a distance of at least 200 meters. Ensure that no one enters the cordoned area. Establish an ICP on the cordon to control access and relinquish ICP responsibility to the military law enforcement authorities or local police upon their arrival. Maintain the cordon until the military law enforcement authorities or local police have completed their examination or state that the cordon may stand down. The decision to allow re-occupation of an evacuated facility rests with the cognizant commander or senior DOD civilian in charge of the facility.

3. Reaction to an Exploded IED

a. **Explosion Without Casualties**

- Maintain the cordon. Allow only authorized personnel into the explosion area.
- Fight any fires threatening undamaged buildings if this can be achieved without risking personnel.
- Report the explosion to the military law enforcement authorities or local police if they are not yet in attendance.
- Report the explosion to the installation operations center even if an EOD team is on its way. Provide as much detail as possible (e.g., time of explosion, number of explosions, color of smoke, and speed and spread of fire).
- Ensure that a clear passage for emergency vehicles (e.g., fire trucks, ambulances) and corresponding personnel is maintained.
- Refer media inquiries to the PAO at the operations center.

- Establish an information center to handle inquiries from the concerned friends and relatives.

b. **Explosion With Casualties.** The first consideration is the effective, organized search for and evacuation of casualties. People naturally approach the explosion area to aid in searching for casualties. The senior officer must coordinate the search and keep the number of searchers to the absolute minimum because of the threat of IEDs and secondary effects (e.g., falling masonry and fires). Attempt to prepare an accurate casualty list for notification of next of kin. It is far better to release an accurate list of casualties a little later than an incorrect list immediately. Arrange for unaffected personnel to quickly contact their next of kin.

c. **Assisting the Threat Management Team**

- Pass available information to the operations center. Do not delay reports because of lack of information — report what you know. Do not take risks to obtain information.

- Include the following information in your report:

  •• Any warning received and if so, how it was received.

  •• Identity of the person(s) who discovered the device.

  •• How the device was discovered (e.g., casual discovery, organized search).

  •• Location of the device — give as much detail as possible.

  •• Time of discovery.

  •• Estimated length of time the device has been in its location.

  •• Description of the device — give as much detail as possible.

  •• Safety measures taken.

  •• Suggested routes to the scene.

  •• Any other pertinent information.

- Access control.

  •• Upon arrival, ensure that military law enforcement authorities, local police, and EOD vehicles are not impeded from reaching the ICP.

  •• Evacuate through building doors and windows.

  •• Obtain a diagram of the building and try to obtain detailed plans of the public service conduits (e.g., gas, electricity, central heating). If unavailable, a sketch can be drawn by someone with detailed knowledge of the building.

  •• Witnesses are invaluable and should be on hand when military and local police arrive. Witnesses include the person(s) who discovered the device, witnessed the explosion, or possesses detailed knowledge of the building or area.

APPENDIX L
JURISDICTIONAL AUTHORITY FOR HANDLING TERRORIST INCIDENTS

JURISDICTIONAL AUTHORITY FOR HANDLING TERRORIST INCIDENTS

LOCATION	INITIAL RESPONSE	PRIMARY AUTHORITY/ JURISDICTION	PRIMARY ENFORCEMENT RESPONSIBILITY	EXERCISING CONTROL OF MILITARY ASSETS	PRIMARY INVESTIGATIVE RESPONSIBILITY
WITHIN THE UNITED STATES					
ON BASE	MILITARY POLICE	FBI/INSTALLATION COMMANDER	FBI/INSTALLATION COMMANDER	INSTALLATION OR UNIT COMMANDER (SUPPORT FBI)	FBI/NCIS/PMO CID/AFOSI
OFF BASE	CIVIL POLICE	FBI/CIVIL POLICE	FBI/CIVIL POLICE		FBI
OUTSIDE THE UNITED STATES					
ON BASE	MILITARY POLICE	HOST GOVERNMENT/DOS INSTALLATION COMMANDER	HOST GOVERNMENT/DOS INSTALLATION COMMANDER	INSTALLATION OR UNIT COMMANDER (IAW APPLICABLE STATUS-OF-FORCES AGREEMENT OR OTHER BILATERAL AGREEMENTS GOVERNING THE EMPLOYMENT OF MILITARY FORCES)	HOST GOVERNMENT/ NCIS/PMO CID AFOSI
OFF BASE	HOST-COUNTRY LAW ENFORCEMENT	HOST GOVERNMENT/DOS	HOST GOVERNMENT/DOS	INSTALLATION OR UNIT COMMANDER (IAW APPLICABLE STATUS-OF-FORCES AGREEMENT OR OTHER BILATERAL AGREEMENTS GOVERNING THE EMPLOYMENT OF MILITARY FORCES)	HOST GOVERNMENT WITH SUPPORT FROM US LAW ENFORCEMENT AGENCIES AS PROVIDED FOR IN BILATERAL AGREEMENTS

NOTE: Coordinate with the local Staff Judge Advocate to clarify authority and questions of jurisdiction. Coordinate with Department of State officials as required. Coordinate in advance with local law enforcement agencies to ensure that support procedures are in place and established information/communication channels are functioning.

LEGEND:

AFOSI	Air Force Office of Special Investigations
FBI	Federal Bureau of Investigation
NCIS	Naval Criminal Investigative Service
PMO	Provost Marshal's Office
CID	Criminal Investigation Division
DOS	Department of State

Figure L-1. Jurisdictional Authority for Handling Terrorist Incidents

APPENDIX M
PUBLIC AFFAIRS CHECKLIST

1. General. Because terrorists seek media recognition, media information management must be in the best interest of the hostage and the situation. The PAO screens information to the media to ensure OPSEC and provides advice and counsel to those in charge. The following checklist contains the planning considerations for the PAO in a crisis management situation.

___ Check with the center commander upon entering the operations center.

___ Revise the public affairs plan to meet the requirements of the situation including a location for the media.

___ Disseminate information to the news media in accordance with the established plan.

___ Control press releases.

___ Coordinate press releases with the commander, staff judge advocate, other operations center staff, and higher echelon PAOs before release.

___ Control movement of news media personnel with press passes and escorts.

___ Obtain approval for the following items from the commander.

— News releases.

— News media personnel to enter outer perimeter.

— Release of photographs of suspects, victims, and immediate scene.

— Interviews with anyone other than the commander.

— Direct communication with press personnel and suspect(s).

2. Focus. The major public affairs focus of the antiterrorist plan should be to ensure that accurate information is provided to the public (including news media) and to communicate a calm, measured, and reasonable reaction to the ongoing event. Commanders should provide the PAO officer with complete control over media activities.

Intentionally Blank

APPENDIX N
MILITARY WORKING DOGS

1. Purpose

This appendix is designed to provide the commander with minimal information concerning the use of MWDs for AT requirements. The military law enforcement office supporting the area should be consulted for specifics associated with using MWDs in the operational area.

2. General

The DOD MWD program produces dual purpose trained MWDs. These MWDs are excellent for use in an AT program. Each Service has MWDs, which are managed and controlled by the law enforcement office at each installation. The MWD program is designed to support tactical operations and daily police commitments. In addition, many host nations have working dog programs that can be used to support military operations. Coordination for host-nation assistance should be done by the local military law enforcement office to ensure compatibility with mission requirements.

3. Advantages

An MWD is a compact, mobile, easily transported asset that can work in a variety of conditions, including confined spaces and difficult terrain. MWDs will increase the speed of many operations and, by their ability to locate explosives and/or firearms at a distance in the right conditions, they can enhance the effectiveness of searches and patrols. The MWD is an excellent deterrent in many circumstances.

4. Disadvantages

An MWD can be distracted by other dogs, animals, people, and food. It can tire, sicken, be injured, reflect the handler's mood, and have inexplicable off-days. Also, an MWD can be affected by extremes in weather. However, with intelligent handling and use many of these disadvantages can be minimized.

5. Antiterrorism Uses

The MWD provides considerable benefit to AT programs. Special forces teams have been known to carry special weapons to eliminate MWDs guarding facilities, thus indicating a strong measure of effectiveness for the inclusion of MWDs in AT plans. The following are some of the possibilities:

a. Patrolling perimeters and critical facilities.

b. Searching for explosives.

c. Augmenting access control points.

d. Serving as a deterrent in riot and crowd control situations.

e. Serving as an early warning indicator for intrusions.

f. Serving as an augmentation to military law enforcement capabilities.

6. Legal Considerations

The military law enforcement office will coordinate with appropriate command legal authorities to determine procedures for MWD in a particular area. These ROE should be spelled out in the AT plan and practiced during training exercises.

Intentionally Blank

APPENDIX O
REFERENCES

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

1. Public Law 99-399, "Omnibus Diplomatic Security and Antiterrorism Act of 1986."

2. DODD 2000.12, "DoD Combating Terrorism Program."

3. DODD O-2000.12H, "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence."

4. DODD 3025.1, "Military Support to Civil Authorities (MSCA)."

5. DODD 3025.12, "Military Assistance for Civil Disturbances (MACDIS)."

6. DODD 3025.15, "Military Assistance to Civil Authorities."

7. DODD 5025.1-M, "DoD Directives System Procedures."

8. DODD 5160.54, "DoD Key Asset Protection Plan (KAPP)."

9. DODD 5210.84, "Security of DoD Personnel at US Missions Abroad."

10. DODD 5240.1, "DoD Intelligence Activities."

11. DODD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons."

12. DODD 5240.6, "Counterintelligence Awareness and Briefing Program."

13. DODD 5525.5, "DoD Cooperation with Civilian Law Enforcement Officials."

14. DODI 2000.14, Draft, "DoD Combating Terrorism Program Procedures."

15. DODI O-2000.16, "DoD Combating Terrorism Program Standards."

16. Defense Special Weapons Agency, Force Protection, Vulnerability Assessment Team, "Guidelines for Assessment Team Members," Initial Draft.

17. Commandant Instruction 16000.12, "Marine Safety Manual," Volumes VII and X.

18. DOD Manual C-5210.41-M, "Nuclear Weapons Security Manual (U)."

19. Joint Pub 0-2, "Unified Action Armed Forces (UNAAF)."

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

21. Joint Pub 1-02, "DOD Dictionary of Military and Associated Terms."

22. Joint Pub 2-0, "Doctrine for Intelligence Support to Joint Operations."

23. Joint Pub 3-0, "Doctrine for Joint Operations."

24. Joint Pub 3-05, "Doctrine for Joint Special Operations."

25. Joint Pub 3-05.3, "Joint Special Operations Operational Procedures."

26. Joint Pub 3-07, "Joint Doctrine for Military Operations Other Than War."

27. Joint Pub 3-07.7, "Joint Tactics, Techniques, and Procedures for Domestic Support Operations."

28. Joint Pub 3-08, "Interagency Coordination During Joint Operations."

29. Joint Pub 3-10, "Doctrine for Joint Rear Area Operations."

30. Joint Pub 3-10.1, "Joint Tactics, Techniques, and Procedures for Base Defense."

31. Joint Pub 3-16, "Joint Doctrine for Multinational Operations."

32. Joint Pub 3-54, "Joint Doctrine for Operations Security."

33. CJCSI 3121.01, "Standing Rules of Engagement for US Forces."

34. CJCSI 3150.25, "Joint After-Action Reporting System."

35. CJCSM 3122.03, "Joint Operation Planning and Execution System Vol II: (Planning Formats and Guidance)."

APPENDIX P
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication to the Joint Warfighting Center, Attn: Doctrine Division, Fenwick Road, Bldg 96, Fort Monroe, VA 23651-5000. 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 Joint Pub 3-07.2, 25 June 1993, "Joint Tactics, Techniques, and Procedures for Antiterrorism."

4. Change Recommendations

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

TO: JOINT STAFF WASHINGTON DC//J34/J7-JDD//

Routine changes should be submitted to the Director for Operational Plans and Interoperability (J-7), JDD, 7000 Joint Staff Pentagon, Washington, DC 20318-7000.

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

c. Record of Changes:

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

5. Distribution

a. Additional copies of this publication can be obtained through Service publication centers.

b. Only approved pubs and test pubs are releasable outside the combatant commands, Services, and Joint Staff. Release of any classified joint publication to foreign governments or foreign nationals must be requested through the local embassy (Defense Attaché Office) to DIA Foreign Liaison Office, PSS, Room 1A674, Pentagon, Washington, DC 20301-7400.

c. Additional copies should be obtained from the Military Service assigned administrative support responsibility by DOD Directive 5100.3, 1 November 1988, "Support of the Headquarters of Unified, Specified, and Subordinate Joint Commands."

By Military Services:

Army:	US Army AG Publication Center SL 1655 Woodson Road Attn: Joint Publications St. Louis, MO 63114-6181
Air Force:	Air Force Publications Distribution Center 2800 Eastern Boulevard Baltimore, MD 21220-2896
Navy:	CO, Naval Inventory Control Point 700 Robbins Avenue Bldg 1, Customer Service Philadelphia, PA 19111-5099
Marine Corps:	Marine Corps Logistics Base Albany, GA 31704-5000
Coast Guard:	Coast Guard Headquarters, COMDT (G-OPD) 2100 2nd Street, SW Washington, DC 20593-0001

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

GLOSSARY

PART I — ABBREVIATIONS AND ACRONYMS

AFOSI	Air Force Office of Special Investigations
AOR	area of responsibility
ASD(C3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
ASD(FMP)	Assistant Secretary of Defense (Force Management Policy)
ASD(SO/LIC)	Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict)
AT	antiterrorism
ATCC	Antiterrorism Coordinating Committee
BAF	backup alert force
C-B	chemical-biological
CIA	Central Intelligence Agency
CINC	commander of a combatant command
CISO	counterintelligence support officer
CJCS	Chairman of the Joint Chiefs of Staff
COM	Chief of Mission
CT	counterterrorism
CTRIF	Combatting Terrorism Readiness Initiative Fund
DIA	Defense Intelligence Agency
DOD	Department of Defense
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
EOD	explosive ordnance disposal
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FCG	Foreign Clearance Guide
FP	force protection
HNS	host-nation support
IAW	in accordance with
ICP	incident control point
IED	improvised explosive device
IR	information requirement

J-2	Intelligence Directorate of a joint staff
JRA	joint rear area
JRAC	joint rear area coordinator
JROC	Joint Requirements Oversight Council
JTF	joint task force
MOOTW	military operations other than war
MOU	memorandum of understanding
MWD	military working dog
NBC	nuclear, biological, and chemical
NCIS	Naval Criminal Investigative Service
NRC	National Response Center
NSC	National Security Council
OP	observation post
OPSEC	operations security
OSD	Office of the Secretary of Defense
OSPG	Overseas Security Policy Group
PAO	public affairs officer
PPBS	Planning, Programming, and Budgeting System
PSYOP	psychological operations
RF	reserve force
ROE	rules of engagement
R&R	rest & recuperation
SAC	special agent in charge
SAL	small arms locker
SAT	security alert team
SDF	self defense force
SOFA	status-of-forces agreement
SOP	standing operating procedure
THREATCON	terrorist threat condition
TSA	travel security advisory
USACIDC	United States Army Criminal Investigations Command
USAMPS	United States Army Military Police School
USCG	United States Coast Guard
USDA&T	Under Secretary of Defense for Acquisition and Technology
VA	vulnerability assessment
WMD	weapons of mass destruction

PART II — TERMS AND DEFINITIONS

aircraft piracy. Any seizure or exercise of control, by force or violence or threat of force or violence or by any other form of intimidation and with wrongful intent, of an aircraft within the special aircraft jurisdiction of the United States. (Joint Pub 1-02)

antiterrorism. Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces. Also called AT. (Joint Pub 1-02)

combatting terrorism. Actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), taken to oppose terrorism throughout the entire threat spectrum. (Joint Pub 1-02)

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

counterintelligence support. Conducting counterintelligence activities to protect against espionage and other foreign intelligence activities, sabotage, international terrorist activities, or assassinations conducted for, or on behalf of, foreign powers, organizations, or persons. (Joint Pub 1-02)

counterterrorism. Offensive measures taken to prevent, deter, and respond to terrorism. Also called CT. (Joint Pub 1-02)

deterrence. The prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction. (Joint Pub 1-02)

force protection. Security program designed to protect Service members, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combatting terrorism, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and other security programs. (This term and its definition replaces the existing term and its definition and is approved for inclusion in the next edition of Joint Pub 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. (Joint Pub 1-02)

hostage. A person held as a pledge that certain terms or agreements will be kept. (The taking of hostages is forbidden under the Geneva Conventions, 1949). (Joint Pub 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. (This term and its definition modifies the existing term and definition and is approved for inclusion in the next edition of Joint Pub 1-02)

incident control point. A designated point close to a terrorist incident where crisis

management forces will rendezvous and establish control capability before initiating a tactical reaction. Also called ICP. (This term and its definition modifies the existing term and definition and is approved for inclusion in the next edition of Joint Pub 1-02)

initial response force. The first unit, usually military police, on the scene of a terrorist incident. (Joint Pub 1-02)

installation. A grouping of facilities, located in the same vicinity, which support particular functions. Installations may be elements of a base. (Joint Pub 1-02)

installation commander. The individual responsible for all operations performed by an installation. (Joint Pub 1-02)

insurgent. Member of a political party who rebels against established leadership. (Joint Pub 1-02)

intelligence. 1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (Joint Pub 1-02)

negotiations. A discussion between authorities and a barricaded offender or terrorist to effect hostage release and terrorist surrender. (Joint Pub 1-02)

open-source intelligence. Information of potential intelligence value that is available to the general public. Also called OSINT. (Joint Pub 1-02)

operations center. The facility or location on an installation, base, or facility used by the commander to command, control, and coordinate all crisis activities. (Joint Pub 1-02)

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

physical security. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material and documents; and to safeguard them against espionage, sabotage, damage, and theft. (Joint Pub 1-02)

prevention. The security procedures undertaken by the public and private sector in order to discourage terrorist acts. (Joint Pub 1-02)

proactive measures. In antiterrorism, measures taken in the preventive stage of antiterrorism designed to harden targets and detect actions before they occur. (Joint Pub 1-02)

status-of-forces agreement. An agreement which defines the legal position of a visiting military force deployed in the territory of a friendly state. Agreements delineating the status of visiting military forces may be bilateral or multilateral. Provisions pertaining to the status of visiting forces may be set forth in a separate agreement, or they may form a part of a more comprehensive agreement. These provisions describe how the authorities of a visiting force may control members of that force and the amenability of the force or

its members to the local law or to the authority of local officials. To the extent that agreements delineate matters affecting the relations between a military force and civilian authorities and population, they may be considered as civil affairs agreements. Also called SOFA. (Joint Pub 1-02)

terrorism. The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. (This term and its definition replaces the existing term and its definition and is approved for inclusion in the next edition of Joint Pub 1-02.)

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

terrorist groups. Any element regardless of size or espoused cause, which repeatedly commits acts of violence or threatens violence in pursuit of its political, religious, or ideological objectives. (Joint Pub 1-02)

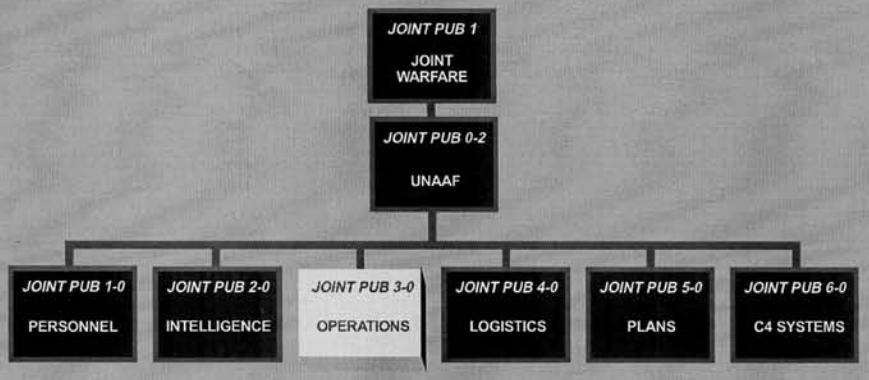
terrorist threat conditions. A Chairman of the Joint Chiefs of Staff-approved program standardizing the Military Services' identification of and recommended responses to terrorist threats against US personnel and facilities. This program facilitates inter-Service coordination and support for antiterrorism activities. Also called THREATCONs. There are four THREATCONs above normal: a. THREATCON ALPHA—This condition applies when there is a general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of THREATCON BRAVO measures. However, it may be necessary to implement certain measures from higher THREATCONs resulting from intelligence received or as a deterrent. The measures in this THREATCON must be capable of being maintained indefinitely. b. THREATCON BRAVO—This condition applies when an increased and more predictable threat of terrorist activity exists. The measures in this THREATCON must be capable of being maintained for weeks without causing undue hardship, affecting operational capability, and aggravating relations with local authorities. c. THREATCON CHARLIE—This condition applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and facilities is imminent. Implementation of measures in this THREATCON for more than a short period probably will create hardship and affect the peacetime activities of the unit and its personnel. d. THREATCON DELTA—This condition applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is likely. Normally, this THREATCON is declared as a localized condition. (Joint Pub 1-02)

threat analysis. In antiterrorism, threat analysis is 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. (Joint Pub 1-02)

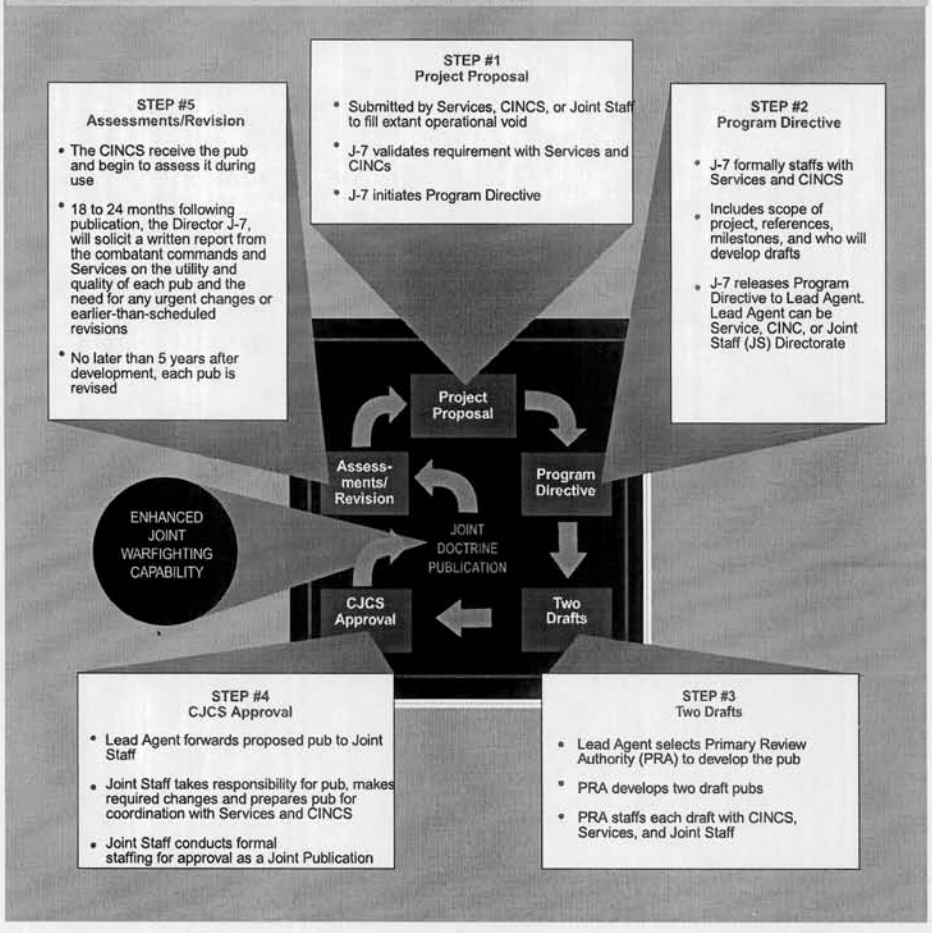
threat and vulnerability assessment. In antiterrorism, the pairing of a facility's threat analysis and vulnerability analysis. (Joint Pub 1-02)

Intentionally Blank

JOINT DOCTRINE PUBLICATIONS HIERARCHY



All joint doctrine and tactics, techniques, and procedures are organized into a comprehensive hierarchy as shown in the chart above. **Joint Pub 3-07.2** is in the **Operations** series of joint doctrine publications. The diagram below illustrates an overview of the development process:




JOINT
CHIEFS OF STAFF