



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301-1400

22 NOV 1993

Ref: 92-FOI-1012

PUBLIC AFFAIRS

Mr. Jeffrey T. Richelson
5 West Glebe Road, C-24
Alexandria, VA 22305

#556

Dear Mr. Richelson:

This responds to your Freedom of Information Act (FOIA) request of May 6, 1992. Our interim response of May 19, 1992, refers.

The Organization of the Joint Staff has provided the enclosed documents as responsive to your request.

The Joint Staff advised this Directorate that the denied portions of Joint Pub 2-0 consist of subjective evaluations, opinions and recommendations, release of which would harm the decision making process. Accordingly, Major General Charles T. Robertson, Jr., Vice Director, Joint Staff, an Initial Denial Authority, has determined that the information is exempt from release pursuant to 5 USC 552 (b) (5).

You have a right to appeal General Robertson's decision to deny the information. Any such appeal should offer justification to support reversal of the initial denial and should be forwarded within 60 days of the date of this letter to the Office of the Assistant Secretary of Defense (Public Affairs), Directorate for Freedom of Information and Security Review, Pentagon, Room 2C757, Washington, D.C. 20301-1400.

Minimal assessable fees are waived for this response in this instance.

Sincerely,

W. M. McDonald
Director

Freedom of Information and
Security Review

Enclosures:
As stated

JOINT PUB 3-07.2

93-F-1012
#556



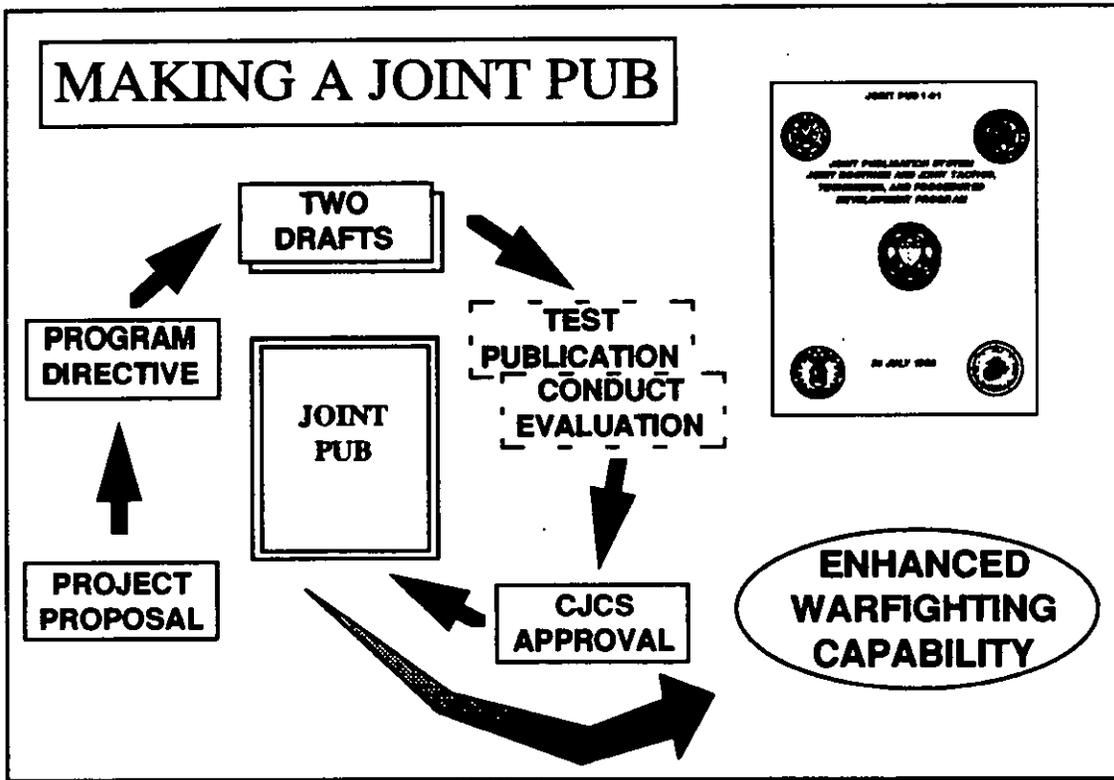
JOINT TACTICS, TECHNIQUES, AND PROCEDURES FOR ANTITERRORISM



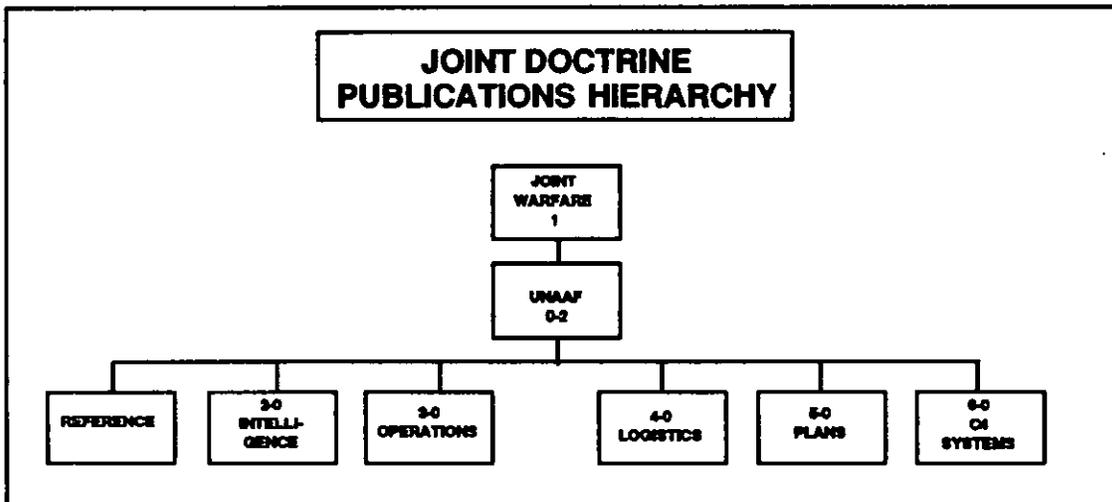
25 JUNE 1993



A large body of joint doctrine (and its supporting tactics, techniques, and procedures) has been and is being developed by the US Armed Forces through the combined efforts of the Joint Staff, Services, and combatant commands. The following chart displays an overview of the development process for these publications.



All joint doctrine and tactics, techniques, and procedures are organized into a comprehensive hierarchy. Joint Pub 3-07.2 is located in the operations series of joint publications.



Joint Pub 1-01, "Joint Publication System," provides a detailed list of all joint publications. Joint pubs are also available on CD-ROM through the Joint Electronic Library (JEL). For information, contact: Joint Doctrine Division, J-7, 7000 Joint Staff Pentagon, Washington, D.C. 20318-7000.



**OFFICE OF THE CHAIRMAN
THE JOINT CHIEFS OF STAFF
WASHINGTON, D.C. 20318-0001**

Reply ZIP Code:
20318-4000

Joint Pub 3-07.2

MEMORANDUM FOR: Distribution List

Subject: Joint Pub 3-07.2, "Joint Tactics, Techniques,
and Procedures for Antiterrorism"

1. This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff. It sets forth the tactics, techniques, and procedures to govern the conduct of joint antiterrorism activities performed by the Armed Forces of the United States.
2. Recommendations for changes to this publication should be submitted to the Director for Operational Plans and Interoperability (J-7), Joint Staff, Washington, D.C. 20318-7000.
3. 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.
4. The Military Services and other Defense agencies are requested to notify the J-7, Joint Staff, when changes to source documents reflected in this publication are initiated.
5. Additional copies of this publication can be obtained through Service publication centers.
6. Local reproduction is authorized.
7. The lead agent for this publication is the US Army.

8. The Joint Staff doctrine sponsor for this publication is the Director for Strategic Plans and Policy, J-5, Joint Staff.

For the Chairman of the Joint Chiefs of Staff:

A handwritten signature in black ink, appearing to read 'T. R. Patrick', written in a cursive style.

T. R. PATRICK
Colonel, USA
Secretary, Joint Staff

Enclosure

Distribution:

Secretary, Joint Staff:

Joint Staff	OSD	NSA	CIA	JWC	USELMNORAD
FEMA	DISA	DIA	DLA	DMA	DNA
NDU	MCCDC	JEWC	AFSC	JDC	DISA-JIEO
CIO					

Additional copies may be obtained from the Secretary, Joint Staff (Documents Division).

Five copies each to: Offices of CSA, CNO, CSAF, CMC, USCG

Twenty-five copies each to:

USLANTCOM	USCENTCOM	USEUCOM	FORSCOM
USPACOM	USSOUTHCOM	USSPACECOM	
USSOCOM	USSTRATCOM	USTRANSCOM	

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,
2800 Eastern Boulevard, Baltimore, MD 21220-2898.

Air Force: Air Force Publications Distribution Center,
2800 Eastern Boulevard,
Baltimore, MD 21220-2896.

Navy: CO, Navy Aviation Supply Office,
Distribution Division (Code 03443)
5801 Tabor Ave, Philadelphia, PA 19120-5000.

Marine Corps: Marine Corps Logistics Base,
Albany, GA 31704-5000.

(INTENTIONALLY BLANK)

LIST OF EFFECTIVE PAGES

The following is a list of effective pages, after the attached pages have been inserted to replace (or add to) the corresponding superseded pages and any deletions made. Use this list to verify the currency and completeness of your document. Substitute this page in your document as a changed page. An "O" indicates a page in the original document.

PAGE	CHANGE	PAGE	CHANGE
i thru xii	O	E-1 thru E-6	O
I-1 thru I-4	O	F-1 Thru F-4	O
II-1 thru II-10	O	G-1 thru G-6	O
III-1 thru III-14	O	H-1 thru H-6	O
IV-1 thru IV-14	O	J-1 thru J-18	O
V-1 thru V-10	O	K-1 thru K-6	O
VI-1 thru VI-10	O	L-1 thru L-2	O
VII-1 thru VII-14	O	M-1 thru M-2	O
A-1 thru A-16	O	N-1 thru N-2	O
B-1 thru B-10	O	O-1 thru O-6	O
C-1 thru C-6	O	GL-1 thru GL-8	O
D-1 thru D-8	O		

Deleted pages: None.

**JOINT TACTICS, TECHNIQUES, AND PROCEDURES
FOR ANTITERRORISM**

PREFACE

1. Purpose. 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 guidance on how to organize, plan, and train for the employment of US forces in interagency and multinational antiterrorism operations.

2. Application

a. Joint tactics, techniques, and procedures (JTTP) established in this publication apply to the commanders of combatant commands, subunified commands, and joint task forces, and their subordinate components. These joint tactics, techniques, and procedures 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, under criteria set forth in Joint Pub 0-2, "Unified Action Armed Forces (UNAAF)."

b. US military and DOD civilians face a continuous threat from a multitude of terrorists, organizations, and individuals using terrorist tactics for criminal, or political gain. For antiterrorism operations to be successful, a joint, combined and interagency effort is essential. DOD personnel at all levels should understand terrorism operations in order to plan effective protective measures to reduce the probability of a successful attack against installations, units, or personnel. This publication defines general command and control relationships and offers organizational examples for potential antiterrorism operations. The publication is authoritative but not directive. Commanders should exercise judgment in applying the procedures herein to accomplish their missions. The JTTP should 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 content of Service publications, this publication will take precedence for activities of joint forces unless the Chairman of the Joint Chiefs of Staff, normally in consultation with other members of the Joint Chiefs of Staff, has provided more current and specific guidance.

c. In applying the doctrine set forth in this publication, care must be taken to distinguish between distinct but related responsibilities in the two channels of authority to forces assigned in combatant commands. The Military Departments and Services recruit, organize, train, equip, and provide forces for assignment in combatant commands and administer and support those forces. Commanders of the unified and specified commands exercise combatant command (command authority) over these assigned forces. Service component commanders are responsible both to joint force commanders in the operational chain of command and to the Military Departments and Services in the chain of command for matters that the joint force commander has not been assigned authority.

3. Scope. This publication is designed to consolidate existing information on antiterrorism for use in the protection of US forces and equipment. This publication is not intended to be a single source antiterrorism document. Service and other Government agency publications provide specific procedures for implementing the guidance provided in this publication in the areas of planning, organizing, training, resourcing, and employing forces for antiterrorism operations.

4. Basis. This publication supports the doctrinal precepts and generally falls under the umbrella of operations described in Joint Pub 3-07, "Doctrine for Joint Operations in Low-Intensity Conflict (LIC)." This publication also draws from a wide variety of documents to outline the foundation for this publication. These include:

- a. "Omnibus Diplomatic Security and Antiterrorism Act of 1986."
- b. DOD Directive O-2000.12, 27 August 1990, "DoD Combatting Terrorism Program."
- c. DOD Manual C-5210.41-M, September 1987, "Nuclear Weapons Security Manual (U)."
- d. Joint Pub 0-1, (in development), "Basic National Defense Doctrine."
- e. Joint Pub 0-2, 1 December 1986, "Unified Action Armed Forces."
- f. Joint Pub 1-01, 30 July 1992, "Joint Publication System, Joint Doctrine and Joint Tactics, Techniques, and Procedures Development Program."

Joint Pub 3-07.2

- g. Joint Pub 1-02, 1 December 1989, "DOD Dictionary of Military and Associated Terms."
- h. Joint Pub 2-0, 30 June 1991, "Doctrine for Intelligence Support to Joint Operations."
- i. Joint Pub 3-0, 1 January 1990, "Doctrine for Joint Operations."
- j. Joint Pub 3-05, 28 October 1992, "Doctrine for Joint Special Operations."
- k. Joint Pub 3-05.3, 30 May 1983, "Joint Special Operations Operational Procedures."
- l. Joint Pub 3-54, 21 August 1991, "Joint Doctrine for Operations Security."
- m. Joint Pub 3-07, (test pub), "Doctrine for Joint Operations in Low Intensity Conflict."
- n. Joint Pub 3-10, (in development), "Doctrine for Joint Rear Area Operations."
- o. Joint Pub 5-03.2, 10 March 1992, "Joint Operation Planning and Execution System Volume II (Planning and Execution Formats and Guidance)."
- p. SM-846-88, 28 October 1988, "Peacetime Rules of Engagement for US Forces (U)."

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

CHAPTER	PAGE
I INTRODUCTION	I-1
General	I-1
Purpose	I-1
Antiterrorism	I-1
Counterterrorism	I-1
Force Protection and Antiterrorism Relationship ...	I-1
Overview of DOD Responsibility	I-2
DOD Role	I-2
The Assistant Secretary of Defense (Special Operations and Low Intensity Conflict)	I-2
The Chairman of the Joint Chiefs of Staff or Designee	I-3
Theater Combatant Commanders	I-3
The Directors of Intelligence and Counterintelligence Components	I-4
Specialized DOD forces	I-4
II TERRORIST THREAT	II-1
Overview	II-1
Terrorist Tactics	II-1
Assassination	II-1
Arson	II-1
Bombing	II-1
Hostage Taking	II-2
Kidnapping	II-2
Hijacking or Skyjacking	II-2
Seizure	II-2
Raids or Attacks on Facilities	II-2
Sabotage	II-2
Hoaxes	II-2
Use of Special Weapons	II-3
Environmental Destruction	II-3
Terrorist Groups	II-3
Non-State-Supported	II-4
State-Supported	II-4
State-Directed	II-4
Terrorist Organization	II-4
Terrorist Targets--Americans	II-7
Domestic Terrorism	II-8
III COMBATTING TERRORISM	III-1
General	III-1
US Policy	III-1

Lead Agencies	III-2
SECTION A. LEGAL CONSIDERATIONS: AUTHORITY	III-2
Criminal Actions	III-2
Jurisdiction	III-3
Commander's Authority	III-3
SECTION B. LEGAL CONSIDERATIONS: CONSTITUTIONAL AND STATUTORY GUIDANCE	III-3
General	III-3
Constitutional Exceptions Allowing the Use of the Military	III-3
Emergency Authority	III-4
Protection of Federal Property and Functions ..	III-4
Statutory Exceptions Allowing the Use of the Military	III-4
Vicarious Liability	III-6
SECTION C. LEGAL CONSIDERATIONS: JURISDICTION AND AUTHORITY FOR HANDLING TERRORIST INCIDENTS	III-7
Jurisdictional Status of Federal Property	III-7
Federal Authority	III-8
Federal and State Concurrent Authority	III-8
SECTION D. LEGAL CONSIDERATIONS: FEDERAL AGENCIES AND THE MILITARY	III-9
Overview	III-9
The National Security Council	III-9
The Committee To Combat Acts of Terrorism	III-9
Department of Justice	III-10
Federal Bureau of Investigation	III-10
Department of Defense	III-10
Military Authority	III-11
Military Installation Commander's Responsibilities	III-11

IV ANTITERRORISM PROGRAM	
UNIT, BASE, PORT, AND INSTALLATION	IV-1
Program Concept	IV-1
Command and Control	IV-1
Antiterrorism Program	IV-1
Antiterrorism Program Concept	IV-2
Six-Step Concept	IV-3
Threat Analysis	IV-4

	Threat Assessment (Criticality and Vulnerability Assessment)	IV-4
	Prevention	IV-5
	Authority and Jurisdiction	IV-9
	Planning Crisis Management	IV-9
	Performing Crisis Management Operations	IV-9
	Implementing the Concept	IV-9
	Installation Commanders	IV-9
	Preventive Planning	IV-10
	Crisis Management Planning	IV-10
	Tenant and Transient Commanders	IV-12
	Threat Conditions	IV-13
	Combatant Commander's Responsibility	IV-13
V	INTELLIGENCE, COUNTERINTELLIGENCE, AND THREAT ANALYSIS	V-1
	SECTION A. INTELLIGENCE AND COUNTERINTELLIGENCE .	V-1
	Intelligence and Counterintelligence Support	V-1
	Sources	V-1
	Open Source Information	V-1
	Criminal Information	V-1
	Government Intelligence	V-2
	Local Information	V-2
	Responsibilities of US Government Lead Agencies ...	V-2
	Essential Elements of Friendly Information	V-5
	SECTION B. THREAT ANALYSIS AND ASSESSMENT.....	V-6
	Preparation of Threat Analysis	V-6
	Drills and Exercises	V-10
VI	CRISIS MANAGEMENT EXECUTION	VI-1
	General	VI-1
	Initial Response	VI-1
	Initial Response Force	VI-1
	Installation, Base, Unit, or Port Commander ...	VI-2
	The Operations Center	VI-2
	Confirmation	VI-2
	Response	VI-3
	Phase I	VI-3
	Phase II	VI-3
	Phase III	VI-3
	Response Sequence	VI-4
	Special Considerations	VI-6
	Establishing and Controlling Communications ...	VI-6
	Evidence	VI-6
	Logistics	VI-7

Disposition of Apprehended Personnel	VI-7
Reports	VI-7
Public Affairs	VI-7
Immediate Post Incident Actions.	VI-9
After-Action Reporting	VI-9

VII PREVENTIVE MEASURES AND CONSIDERATIONS VII-1

Commander's Responsibility	VII-1
Protecting Deployed Forces in High-Risk Areas ...	VII-1
Installations, Bases, Sites, and Nonurban	
Facilities	VII-1
Guard Duties	VII-6
Road Movement	VII-7
Vehicle Protection	VII-7
Convoys	VII-8
Rail Movement	VII-9
Sea Movement	VII-10
Air Movement	VII-10
Patrolling	VII-11
Roadblocks	VII-12
Observation Posts	VII-12
Civil Disturbances	VII-12
Bomb Explosion or Discovery	VII-13
Personal Protective Measures	VII-13
Tactical Force Protection	VII-13

APPENDIX

A Vulnerability Assessment	A-1
B Personal Protective Measures Against Terrorism ...	B-1
C VIP and Senior Officer Security Measures	C-1
D Office 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 Users Evaluation Report	O-1

Glossary

Part I--Abbreviations and Acronyms	GL-1
Part II--Terms and Definitions	GL-4

TABLE

IV-1	Antiterrorism Program Functions	IV-10
IV-2	Crisis Management Participants	IV-11
IV-3	On-Site Operational Response Structure	IV-12
V-I	Threat Level.....	V-8
VII-1	Fortification Materials	VII-4
VII-2	Security Force Equipment	VII-5

FIGURE

II-1	Structure Pyramid	II-5
IV-1	Antiterrorism Program Concept	IV-3
VI-1	Response to a Terrorist Incident	VI-5

(INTENTIONALLY BLANK)

CHAPTER I

INTRODUCTION

1. General. The term "terrorism" is defined in DOD Directive O-2000.12, 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 and directive guidance for the DOD Combatting Terrorism Program is contained in DOD Directive O-2000.12.

2. Purpose. Combatting terrorism involves actions, including antiterrorism (defensive measures used to reduce the 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. This publication addresses only antiterrorism. The following definitions are provided to assist in understanding the difference between antiterrorism and counterterrorism.

a. Antiterrorism includes defensive measures used to reduce the vulnerability of individuals and property to (Joint Pub 1-02) . . . terrorist acts, to include limited response and containment by local military forces. (DOD Directive O-2000.12) The latter portion will be added to the original definition to clarify the definition's scope. This publication uses the expanded DOD antiterrorism definition.

b. Counterterrorism involves those offensive measures taken to prevent, deter, and respond to terrorism. Sensitive and compartmented counterterrorism programs are addressed in relevant National Security Decision Directives (NSDDs), National Security Directives (NSDs), contingency plans, and other relevant classified documents.

3. Force Protection and Antiterrorism Relationship. Antiterrorism, as discussed throughout this publication, is an element of a broader concept called force protection. In Joint Pub 5-03.2, the term "force protection" is described as a security program designed to protect soldiers, civilian employees, family members, facilities, and equipment in all locations and situations. This is accomplished through planned and integrated application of combatting terrorism, physical security, operations security (OPSEC), personal protective

services, supported by intelligence, counterintelligence, and other security programs.

4. Overview of DOD Responsibility. As discussed in Joint Pub 5-03.2, 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. 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 antiterrorism 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.

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, deployed forces, equipment and installations. At times, the Department of Defense is responsible for providing technical assistance or forces when directed or requested by the lead agency. The lead agency is either the DOS for incidents outside the United States, or the Department of Justice (DOJ) for incidents within the United States, or the Federal Aviation Administration (FAA) for certain aviation incidents. The following DOD offices and agencies have been assigned specific responsibilities pertaining to combatting terrorism:

a. The Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict) or Designee. This official performs the following functions concerning terrorism matters:

- (1) Monitors, with other DOD components, the programs to reduce the vulnerability of DOD personnel, their family members, facilities, and other resources from terrorist acts.
- (2) Represents the Secretary of Defense on interagency committees concerning terrorism matters.
- (3) Chairs the DOD Antiterrorism Coordinating Committee meeting.

(4) Develops, publishes, and maintains the DOD Directive O-2000.12 to provide guidance on protective measures that reduce the vulnerability of DOD personnel, their families, and facilities to terrorism.

(5) Coordinates with the Assistant Secretaries of Defense for International Security Affairs and International Security Policy for issuance and update of the DOD travel security advisory message.

(6) Provides policy oversight and guidance to DOD components in support of antiterrorism efforts.

(7) Acts as DOD point of contact for matters relating to sharing data and information on antiterrorism and the threat posed by domestic and foreign terrorists to the Department of Defense.

b. The Chairman of the Joint Chiefs of Staff or Designee.
The Chairman performs the following antiterrorism functions:

(1) Ensures that unified and specified command policies and programs are established for protection of DOD personnel, their families, facilities, and other resources from terrorist acts.

(2) Implements the DOD Terrorist Threat Conditions (THREATCONs) System consistent with DOD Directive O-2000.12.

(3) Provides a representative on DOD committees concerning terrorism matters.

c. Theater Combatant Commanders. The combatant commanders perform the following antiterrorism measures:

(1) Through their chain of command, create a level of awareness, appreciation, and readiness commensurate to the threat.

(2) Ensure proper coordination of all local policies and measures for protecting DOD facilities, resources, equipment, personnel, and family members in foreign areas from terrorist acts and for assisting their subordinate commanders in implementing Military Service programs.

(3) Ensure that the DOD THREATCONS for combatting terrorism are uniformly implemented as specified in DOD Directive O-2000.12.

(4) Serve as the DOD point of contact with US embassies and host-nation officials on matters regarding such policies and measures. This includes serving on each DOS regional liaison group. Theater CINCS, with the concurrence of the host-nation US Ambassador, train host-nation military forces for antiterrorism and combatting terrorism missions. For a complete understanding of this relationship and interface, see US DOS FAH-1 EPH and applicable CINC plans.

(5) Assess the terrorist threat for the theater and provide a copy of the threat assessment to the Services. On the basis of the threat assessment, identify and recommend to the appropriate authority those incumbents of high-risk billets and adult family members requiring training en route to the assignment. Chapter IV provides details concerning available training.

d. The Directors of Intelligence and Counterintelligence Components. These directors of components of the Military Services, Defense Intelligence Agency (DIA), and National Security Agency (NSA), or their designees ensure prompt dissemination of intelligence information, including specific warnings. Information on terrorist threats is disseminated routinely by the Military Services, DIA, and NSA to DOD members traveling in threat areas.

e. Specialized DOD Forces. The counterterrorist JTF provides a flexible range of responses to deal with terrorist threats.

CHAPTER II

TERRORIST THREAT

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 sufficient background information concerning the terrorist threat to enable the commander at any echelon to properly create and employ antiterrorism tactics, techniques, and procedures outlined in this publication. Terrorism has become a media event and, as such, a phenomenon of our time. This is why news media coverage is important to terrorists who are attempting to excite 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. Operations to meet the threat may fall in both the counterterrorism and antiterrorism arenas. It 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 some vague cause and/or remote political group to give their actions a claim to respectability.

2. Terrorist Tactics. Examples of objectives that a terrorist attack may be associated with, but not limited to, are as follows: 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 contemporary terrorist groups are:

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

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

c. Bombing. The improvised explosive device (IED) is the contemporary 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. 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 1990, 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 when executed in an unfriendly environment.

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. The 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 for logistic purposes; e.g., robbery of a bank or armory.

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

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. Although chemical and biological weapons have not been widely used by terrorists to date, there is a potential for their use and threat thereof. 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 device using nuclear contaminants as a weapon 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. Danger in handling and fear of alienation by peer and support groups has probably inhibited the use of chemical and biological weapons by terrorist groups to date. This situation could change as the competition for headlines increases.

l. Environmental Destruction. Although this tactic has not been widely asserted, 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. The fear of alienation may also be a factor that has limited the use of this tactic to date.

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. Ease of international travel and the growing tendency toward cooperative efforts among terrorist groups have made categorization of terrorist groups more difficult, but the terms are still helpful in the identification process. 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:

- a. Non-State-Supported. A terrorist group that operates autonomously, receiving no significant support from any government; e.g., Italy's Red Brigade.
- b. State-Supported. A terrorist group that generally operates independently but receives support from one or more governments; e.g., Popular Front for the Liberation of Palestine.
- c. State-Directed. A terrorist group that operates as an agent of a government, receiving substantial intelligence, logistic, and operational support from the sponsoring government; e.g., Abu Nidal organization.

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. Organizations such as the Red Army Faction and Red Brigade 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 decisionmakers, 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-1, a typical organization consists of operational members who are functionally organized as outlined above and 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.

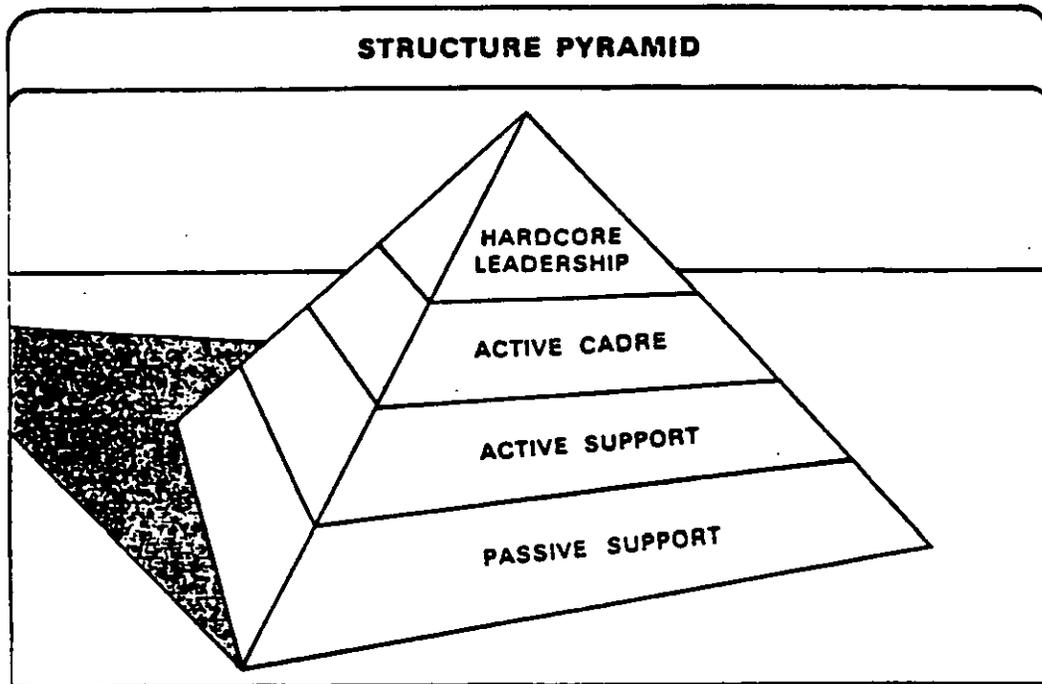


Figure II-1. Structure Pyramid

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. Therefore, many individuals responsible for terrorist acts could fit into one of three categories: crusaders, criminals, or emotionally disturbed. A specific individual may exhibit traits from more than one category. Terrorists look like ordinary citizens and come from all walks of life.

(1) 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.

(2) 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 hard skills (e.g., auto theft, forgery, weapon handling, bomb making), that were acquired before entering the group.

(3) 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. 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.

e. The active, operational cadre are the doers--the men and women who carry out terrorist attacks and train others. As 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.

f. 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.

g. Passive supporters are more difficult to define and, in practice, more difficult to identify. Most of these people are sympathetic to the terrorist group's cause but either cannot or will not assume an active role. 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 support them. Thus, fear rather than sympathy generates support for the terrorist. The terrorist group relies on passive supporters for financial assistance, displays of public support, and minor logistic or operational tasks.

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 excite 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 pervasive 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 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. Although the United States has one of the highest levels of social violence in the world, the incidence of terrorism in the United States has remained very low compared to Europe, Latin America, Africa, or the Middle East. There are several reasons for this seeming inconsistency. 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. As long as there are opportunities for success through this process, with no proscribed political groups, domestic terrorism is likely to remain limited.

a. 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 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.

b. Terrorism is a factor across the entire operational continuum. 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 hostilities short of war; however, in war the threat of terrorism is only one of many force protection 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.

c. 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, etc.), 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, etc.) or has a high symbolic value (headquarters, particular individuals, etc.), the crime probably has terrorist implications even when no claim is forthcoming. Recognizing the difference between acts of violence and terrorist acts is vital to properly understanding the threat's intent and determining required defensive measures. Chapter III, Section A, provides further information concerning prosecution of terrorist acts during peacetime military operations and war.

(INTENTIONALLY BLANK)

CHAPTER III

COMBATting TERRORISM

1. General. This chapter explains the importance and necessity for participation of a command legal adviser at all levels of foreign and domestic antiterrorism program planning and implementation. It is designed to provide the commander of a combatant command, subunified command, JTF, or component command sufficient basic understanding of the legal considerations affecting the successful implementation of an effective program in order to properly use the chief legal adviser. The policy and jurisdictional responsibilities generally applicable to the US Armed Forces 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 blackmail 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. However, 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

- a. DOS is the lead agency for response to terrorism outside the United States.
- b. DOJ is normally the lead agency for domestic terrorism; the FBI is the lead agency within DOJ for operational response to terrorist incidents.
- c. FAA is the lead agency for terrorist incidents that occur aboard an aircraft in flight. It is 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. 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. USCG is the lead agent responding to terrorist actions that occur in maritime areas subject to US jurisdiction (14 USC, 89). Additionally, the USCG and FBI have an interagency agreement (Commandant Instruction 16202.3A) to cooperate with each other when coordinating counterterrorism activities.
- 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 peacetime military operations, hostilities short of war, or war; however, jurisdiction varies in wartime. Terrorists, by definition, 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 military operations, terrorist acts are punishable under domestic (local) law. This is also true in police actions to maintain a legitimate government. However, in an internationally recognized war or hostilities short of war (regional or global), terrorists can be tried under local criminal law or under military jurisdiction by either a court-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 legal advisers to determine the extent of their authority to combat terrorism.

**SECTION B. LEGAL CONSIDERATIONS:
CONSTITUTIONAL AND STATUTORY GUIDANCE**

7. General. 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 1835) and in SECNAVINST 5820.7 (series) for the Navy and Marine Corps, and in AFR 110-3, Chapter 16, for the Air Force, and in the addition of Chapter 18 to 10 USC 371 through 378. These restrictions do not apply in foreign countries or to actions on military bases or in military-contracted buildings or spaces, or in guarding military property in-transit for primarily military purposes. The Posse Comitatus Act has been interpreted as 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 provided by statute, to assist local law enforcement officers in carrying out their duties. The same prohibition applies 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; however, constitutional exceptions do permit the US Government to use military forces to preserve law and order within its territorial limits.

8. Constitutional Exceptions Allowing the Use of the Military. The constitutional authority that applies to these exceptions is based on the inherent legal right of the US Government to ensure

the preservation of public order and continued governmental functioning within its territorial limits, by force if necessary. These exceptions include:

a. Emergency Authority. This authorizes prompt and vigorous Federal action, including the use of military forces, to prevent loss of life or wanton destruction of property and to restore governmental functioning and public order when sudden and unexpected civil disturbances, disasters, or calamities seriously endanger life and property and disrupt normal governmental operations to such an extent that duly constituted local authorities are unable to control the situation.

b. Protection of Federal Property and Functions. This authorizes Federal actions, including use of military forces, to protect Federal property and functions when the need for protection exists and duly constituted local authorities are unable or decline to provide adequate protection. (DOD Directive 3025.12, "Employment of Military Resources in the Event of Civil Disturbances," paragraph V.C., 19 August 1971, as amended, and DOD Directive 5160.54, 26 June 1989, "DoD Key Asset Protection Plan (KAPP)."

9. Statutory Exceptions 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 federalized forces; i.e., National Guard, to enforce the laws. To illustrate, the President is currently empowered to use military forces:

a. To restore and maintain public order:

(1) 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, he may use Federal armed forces as he deems necessary to enforce those laws or to suppress the rebellion under the statute (10 USC 332).

(2) 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 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 as he deems necessary, to suppress such disturbances.

(3) Whenever the President considers it necessary to use the National Guard or Federal armed forces under the authority of the intervention statutes discussed above, he 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. (DOD Directive 3025.12, paragraph V.C.2a, as amended).

(4) Emergency use of military aircraft in air piracy or aircraft hijacking cases may be authorized by the National Military Command Center (NMCC) (Deputy Secretary of Defense memorandum, 29 June 1972, "Support of Civil Authorities in Airplane Hijacking Emergencies"). Military aircraft may be committed for use as chase planes.

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

b. To meet specified contingencies:

(1) 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))).

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

(3) To assist the Attorney General in enforcing drug abuse prevention and control (21 USC 873(b)).

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

(5) 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 the calamity or extreme emergency renders it dangerous to wait for instructions from the proper military department, a commander may take whatever action the circumstances reasonably justify. However, the commander must comply with the following:

(1) Report the military response to higher headquarters.

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

(3) Retain military response under the military chain of command.

(4) Limit military involvement to the minimum demanded by necessity.

(5) Emergency situations include, but are not limited to, the following:

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

b. Providing emergency explosive ordnance disposal (EOD) service.

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

10. Vicarious Liability. Commanders at all echelons should be aware of the legal principle of vicarious liability in planning and implementing antiterrorist measures. This principle imposes indirect legal responsibility upon commanders for the acts of subordinates or agents. For example, willful failure on the part of the commander or a subordinate to maintain a trained

and ready reaction force as required by regulation, could be construed as an act taking the commander out of the protected position found in being an employee of the Federal Government; thus making the commander subject to a civil suit by any hostages injured. Civil or criminal personal liability may result from unlawful acts, negligence, or failure to comply with statutory guidance by subordinates or agents. With the increasing number of civilian contract personnel on military installations and the sophistication of terrorist organizations, commanders should pay particular attention to meeting regulatory requirements and operating within the scope of their authority. The legal principle of vicarious liability, long established in the civilian community, has only recently applied to the military community. In this light, the command legal adviser has become increasingly important to the commander in the planning, training, and operational phases of the antiterrorist program.

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

11. Jurisdictional Status of Federal Property. 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.

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. The Assimilative Crimes Act, 18 USC 13, however, 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 United States 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 United States 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. The Federal Government may, however, prosecute violations of state law under the Assimilative Crimes Act.

d. Proprietorial jurisdiction means that the United States 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.

12. Federal Authority. 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 purposes. The Federal law contains no special prohibition against terrorist acts or threats, as do some state codes. The Assimilative Crimes Act, however, 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.

13. 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.
- b. The importance of the state or Federal interest sought to be protected under the criminal statute.

14. The matrix in Appendix L 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

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

16. The National Security Council. The NSC formulates US policy for dealing with terrorist acts and advises the President on terrorist threats that endanger US interests.

17. 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 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, DOD or other US agencies may be invited to provide assistance if American interests are involved. In such cases, the US Chief of Mission oversees the activities of US agencies.

18. Department of Justice. DOJ is normally 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.

19. 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 materiel, or dangerous radioactive materiel. 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.

20. Department of Defense. DOD Directive O-2000.12 prescribes that the Assistant Secretary of Defense (Special Operations and Low Intensity Conflict) (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:

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

For the military planner in the United States, its territories and possessions, this relationship between DOJ and the 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. These local agreements, because of military turnover and reorganization, should be reviewed and tested annually.

21. Military Authority. 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 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.

22. 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. Contingency 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:

(1) 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.

(2) If the FBI assumes jurisdiction, the Attorney General will assume primary responsibility for coordinating the Federal law enforcement response.

(3) If the FBI declines jurisdiction, the senior military commander will take action to resolve the incident.

(4) 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.

(5) In all cases, command of military elements remains within military channels.

(6) Response plans with the FBI and Service agencies should be exercised annually at the installation and base level to ensure 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 DOS is made at the theater combatant commander level. In all theaters, existing contingency plans provide guidance to the installation commander regarding notification procedures. 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 peacetime rules of engagement (ROE), 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 (SM-846-88).

(1) 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 memorandums of understanding (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 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.

(2) Antiterrorism plans should:

(a) Be required by the Chairman of the Joint Chiefs of Staff for implementation by theater, combatant commands, subunified commands, JTFs, and component commands.

(b) Be coordinated with and approved by the theater combatant commander or his designated representative.

(c) 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."

(d) Be coordinated with both host-nation and DOS officials.

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

(INTENTIONALLY BLANK)

CHAPTER IV

ANTITERRORISM PROGRAM

UNIT, BASE, PORT, AND INSTALLATION

1. Program Concept. To meet the terrorist threat, an integrated and comprehensive antiterrorism 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.

a. Command and Control. When terrorists attack a DOD target, the NMCC becomes the command post for the Joint Staff and the Secretary of Defense. The command, control, and reporting responsibilities for foreign terrorist attacks on DOD targets belong to the theater combatant commander within whose area of responsibility the attack has occurred. Combatant command reporting will use the National Military Command System (NMCS). Domestic terrorist attacks on DOD targets will be reported by the Service or agency in command of the targeted installation.

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

- (1) Threat analysis.
- (2) Installation or unit criticality and vulnerability assessments.
- (3) Creation of a threat assessment based on the threat analysis and friendly vulnerabilities.
- (4) Operations security (OPSEC).
- (5) Personnel security.

- (6) Physical security.
- (7) Crisis management planning.
- (8) Employment of tactical measures to contain or resolve terrorist incidents.
- (9) Continuous training and education of personnel.
- (10) Public affairs planning.

c. Antiterrorism Program Concept. 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. 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 integration of the installation's physical assets, force 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.

ANTITERRORISM PROGRAM CONCEPT

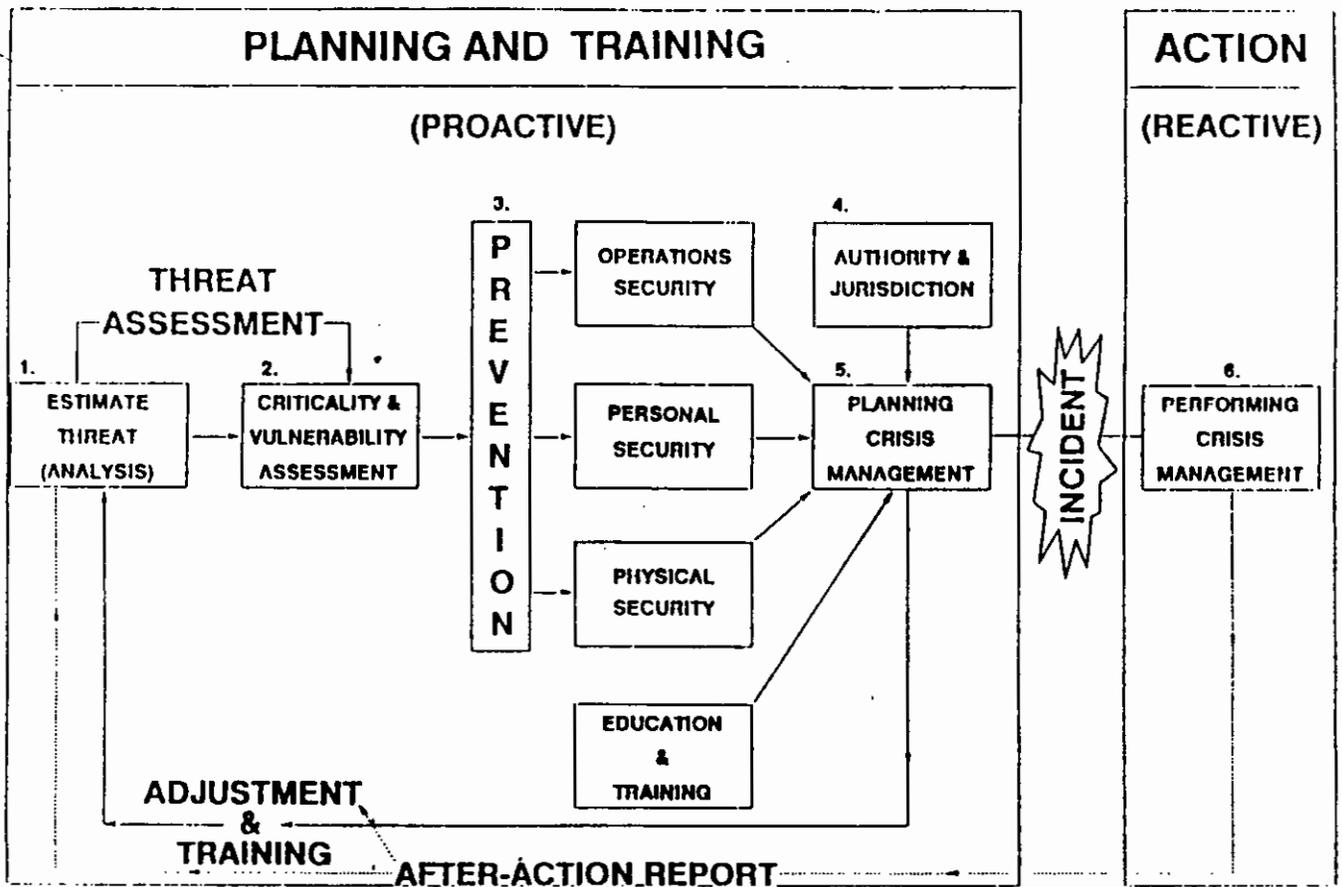


Figure IV-1. Antiterrorism Program Concept

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. The crisis management phase is discussed in Chapter VI.

(1) Threat Analysis. A threat analysis must be current; as data for the estimation changes, so does the risk. Of critical importance in this 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. The basic steps in the criminal information and intelligence process are:

(a) 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.

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

(2) Threat Assessment (Criticality and Vulnerability Assessments). The threat assessment brings together the threat analysis and the vulnerability analysis. The threat assessment concerns people or items essential to the mission or function of the installation, port, base, or unit. 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. Based on the threat assessment, the commander and staff should identify and prioritize critical personnel, facilities, and equipment, and should conduct a vulnerability assessment for each (see Appendix A). 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 vulnerability assessment 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 vulnerability assessment at least annually to ensure that it remains accurate in view of the changing threat, installation makeup, and unit missions.

(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.

(a) 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 (COMSEC) 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 antiterrorism are to:

1. Deny intelligence and information to terrorists.
2. Avoid rigid operational routines.
3. Be familiar with techniques used by terrorists to collect information.
4. Integrate OPSEC into physical security and personal protection programs.
5. Develop essential elements of friendly information (EEFI) to facilitate and focus efforts to deny information to terrorists.

(b) 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. A vulnerability assessment may identify specific personnel who, by virtue of their rank, position, travel itinerary, or symbolic value, may become particularly attractive or assessable targets. Prevention of such attacks depends on the planning and the use of the personal protection measures outlined in Appendix C. The

(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.

(a) 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 (COMSEC) 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 antiterrorism are to:

1. Deny intelligence and information to terrorists.
2. Avoid rigid operational routines.
3. Be familiar with techniques used by terrorists to collect information.
4. Integrate OPSEC into physical security and personal protection programs.
5. Develop essential elements of friendly information (EEFI) to facilitate and focus efforts to deny information to terrorists.

(b) 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. A vulnerability assessment may identify specific personnel who, by virtue of their rank, position, travel itinerary, or symbolic value, may become particularly attractive or assessable targets. Prevention of such attacks depends on the planning and the use of the personal protection measures outlined in Appendix C. The

the techniques of personal protection and security commensurate with the threat in his 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 antiterrorism planners; 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. High-risk positions are identified and so designated by the combatant commander based on the following considerations:

a. Location.

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 (INTAC) conducted by US Army John F. Kennedy Special

Warfare Center (USAJFKSWCS), 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, D.C.

3. Protective Training. Personnel en route to potential physical threat risk areas (as identified by the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict) 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 antiterrorism 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 instruction in cultural, political-military, and individual security factors associated with the region.

c. Training may also be given by installation security personnel who have been trained at the Antiterrorism

Instructor Qualification Course (AIQC) at
Fort Bragg, North Carolina.

(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 outlines the responsibilities of the Department of Defense, DOJ, FAA, and DOS in terrorist incidents. Implicit in the jurisdictional definitions is the requirement for the local commander to determine whether an incident is terrorist in nature or the act of a nonterrorist.

(5) Planning Crisis Management. The establishment of a mechanism to respond to a terrorist incident is an essential element of the antiterrorism 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 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.

(6) Performing Crisis Management Operations. As the threat increases, a series of graduated DOD THREATCONs dictate prescribed actions (DOD Directive O-2000.12).

2. Implementing the Concept

a. Installation Commanders. Commanders directly responsible for operating bases, 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 by establishing antiterrorism programs. This responsibility includes the security of personnel, equipment, materiel, and facilities. To implement the antiterrorism program, the installation commander causes functions to be performed as shown in Table IV-1.

Table IV-1. Antiterrorism Program Functions

COMMAND

PREVENTIVE PLANNING

- Awareness Training
- Personal Protection
- Physical Security
- OPSEC
- Drills/Exercises

**CRISIS MANAGEMENT
PLANNING**

- Communications
- Logistics
- Operational Control

- Command
- Initial Response Force
- Special Response Force Augmentation
- Special Response Force Commitment
- Post-Incident Procedures

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 is responsible for developing and coordinating the antiterrorism programs. A threat committee, which is part of the planning organization, is also established to maintain and access current threat information and functions as a working element of the preventive planning organization. This enables the organization to develop a threat assessment, at least annually, based on the information provided by the threat committee. The preventive planning organization should include staff from operations, intelligence, counter-intelligence, law enforcement, engineers, and public affairs. This organization should consider the installation from an antiterrorism 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) to form an organization to plan and coordinate the command's

antiterrorism 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 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 his 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 Table IV-2.

TABLE IV-2. CRISIS MANAGEMENT PARTICIPANTS

- Personnel
- Intelligence/Security
- Operations
- Counterintelligence
- Logistics
- Civil Affairs
- Special Staff Sections:
 - Military Law Enforcement Authorities
 - Command Legal
 - Public Affairs
 - Transportation
 - Aviation
 - Communications
 - Engineers/Utilities
 - Medical Activity/Red Cross
 - Chaplain
 - Psychologist
 - EOD Section
- Major Tenant Commands
- Local Investigative Field Office (CID, NISCOM, etc.)
- Civilian Authorities/Representatives
- Federal, State, Local, or Host-Nation Police

(1) 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 or standard operating procedures (SOPs). As dictated by these SOPs, predetermined and adequate communications systems must be made available at the location. The operational SOPs are stressed and validated during the installation's annual operational antiterrorism evaluation exercise.

(2) 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 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. Table IV-3 illustrates normal functions performed by the operational response force.

Table IV-3. On-Site Operational Response Structure

<u>SECURITY</u>	<u>REACTION/MANAGEMENT</u>	<u>SUPPORT</u>
Military/Security Police (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 Communications Personnel

d. Tenant and Transient Commanders. Commanders who are not under the operational 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 0-2, Chapter 4, paragraph 4-10, apply. Tenant commanders are still responsible for their commands physical security and 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, Chapter 4, paragraph 4-11, apply.

3. Threat Conditions. The mechanism by which the antiterrorism program operationally increases or decreases protective measures is the DOD THREATCON System (Appendix J). 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 antiterrorism 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 combatant commander designates a staff office, usually in the J-3 or law enforcement or security section, to supervise, inspect, test, and report on the base antiterrorism programs within theater. This staff section also coordinates with host-nation authorities and the US Embassy. Simultaneously, the J-2, under the combatant commander's authority, disseminates intelligence on terrorist activities to the subordinate commands to ensure the anti-terrorism measures are appropriate to the threat. The manner in which the combatant commander places importance on these staff functions usually has a direct affect on the antiterrorism readiness of subordinate commands.

(INTENTIONALLY BLANK)

CHAPTER V

INTELLIGENCE, COUNTERINTELLIGENCE, AND THREAT ANALYSIS

SECTION A. INTELLIGENCE AND COUNTERINTELLIGENCE

1. Intelligence and Counterintelligence Support. Intelligence and counterintelligence are the first line of defense in an antiterrorism program. A well-planned, systematic, all-source intelligence and counterintelligence program is essential. The role of intelligence and counterintelligence in antiterrorism is to identify the threat. Additionally, counterintelligence provides warning of potential terrorist attacks and provides information for counterterrorism operations. This chapter provides the reader with the elements of the intelligence cycle that have particular importance in a viable antiterrorism program. Effective intelligence and counterintelligence support requires effort, planning and direction, collection and analysis, production, investigations, and dissemination. The entire process is important to providing decisionmakers with information and timely warning upon which to recommend antiterrorism actions.

2. Sources. The primary sources of intelligence and counterintelligence for the antiterrorism program are open source information, criminal information, government intelligence, counterintelligence, and local information.

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, 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.

b. Criminal Information. Both military and civil law enforcement agencies collect criminal information. Because terrorist acts are criminal acts, criminal information is a major source for terrorist intelligence. Commanders must work through established law enforcement liaison channels because the collection, retention, and dissemination of criminal information are regulated. Local military criminal investigative offices of the US Army Criminal Investigations

Command (USACIDC); Naval Investigative Service Command (NISCOM); Air Force Office of Special Investigations (AFOSI); and Headquarters, US Marine Corps, Criminal Investigations Division (HQMC (CID)), maintain current information that will assist in determining the local terrorist threat.

c. Government Intelligence. The Community Counterterrorism Board (CCB) is responsible for coordinating the national intelligence agencies concerned with combatting international terrorism. These agencies include CIA (lead agency), DIA, NSA, DOS, DOJ, FBI, Department of Energy (DOE), Department of Transportation (DOT) (USCG), FAA, and the Department of Defense. Service intelligence and counterintelligence production organizations include the US Army Intelligence Threat Analysis Center (USAITAC); the Navy Anti-terrorism Analysis Center (NAVATAC); Headquarters, US Marine Corps, Counterintelligence (HQMC(CIC)); and US AFOSI Investigations Operations Center (IOC); that compile comprehensive intelligence and counterintelligence from these agencies for distribution on a need-to-know basis throughout the Services. In combatant commands, the J-2 is responsible for the intelligence fusion center. 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 DOS, DIA, and the host nation are also active players. Military intelligence activities are conducted in accordance with Presidential Executive orders, Federal law, SOFAs, MOUs, and applicable Service regulations.

b. Responsibilities of Intelligence Activities

(1) The combatant commander, through the commander's J-2 and the CISO in consultation with DIA, CIA, embassy staff, country team, and applicable host-nation authorities, obtains intelligence and counterintelligence specific to the area of operation 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 area of operations. This network is the backbone for communicating intelligence and counterintelligence information, advisories, and warning of terrorist threats throughout the region.

(2) In DOD Directive O-2000.12, the Secretaries of the Military Departments were requested to ensure that a capability exists to 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 agency (US Army Intelligence and Security Command (INSCOM), Naval Investigative Service Command (NISCOM), 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:

(a) Coordinates with appropriate US and host-nation agencies.

(b) Provides overall direction and coordination of the Service counterintelligence effort.

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

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

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

(f) Provides terrorist threat information in threat briefings.

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

(h) 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.

(3) Investigative Agencies. Service criminal investigative services (e.g., USACIDC, NISCOM, 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 or security police and civilian law enforcement agencies.

(4) Intelligence staff elements of commanders at all echelons:

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

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

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

(5) Law enforcement staff elements will:

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

(b) Initiate and maintain liaison with local counterintelligence offices and military criminal investigative offices.

(c) Maintain liaison with Federal, host-nation, and local law enforcement agencies or other civil and military antiterrorism agencies as appropriate.

(6) Installation, base, unit, and port security officers:

(a) 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.

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

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

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

4. Essential Elements of Information. To focus the threat analysis, intelligence and counterintelligence officers develop essential elements of information (EEI) to identify likely targets using the following terrorist considerations:

- a. Organization, size, and composition of group.
- b. Motivation.
- c. Long- and short-range goals.
- d. Religious, political, and ethnic affiliations.

- e. International and national support; e.g., moral, physical, financial.
- f. Recruiting methods, locations, and targets; e.g., students.
- g. Identity of group leaders, opportunists, and idealists.
- h. Group intelligence capabilities and connections with other terrorist groups.
- i. Sources of supply and support.
- j. Important dates; e.g., religious holidays.
- k. Planning ability.
- l. Internal discipline.
- m. Preferred tactics and operations.
- n. Willingness to kill.
- o. Willingness for self-sacrifice.
- p. Group skills (demonstrated or perceived); e.g., sniping, demolitions, masquerade, industrial sabotage, airplane or boat operations, tunneling, underwater, electronic surveillance, poisons or contaminants.
- q. Equipment and weapons (on-hand and required).
- r. Transportation (on-hand and required).
- s. Medical support availability.

SECTION B. THREAT ANALYSIS AND ASSESSMENT

5. Preparation of Threat Analysis. The preparation of the terrorist threat analysis is a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups that could target a facility. 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 vulnerability analysis to create the threat and vulnerability assessment. Threat analysis is an essential step in identifying probability of terrorist attack. To enhance the capability to collect and analyze information from many sources, the Military Department lead agency maintains a terrorism data base and the

combatant command's J-2 and 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. From these sources, the lead agency derives worldwide, area, and general threat analyses that are disseminated to appropriate organizations throughout the Service. Commands at all echelons then augment or refine the lead agency threat analyses to focus on their area of interest. This process, operative in all states of the operational continuum, 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 counter-intelligence 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. Key questions are:

(1) What has changed (mission, political climate, installation and unit personnel or equipment, terrorist capabilities)?

(2) 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, accurate threat and vulnerability assessments, 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.

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

- (1) **EXISTENCE:** A terrorist group is present, assessed to be present, or able to gain access to a given locale.
- (2) **CAPABILITY:** The acquired, assessed, or demonstrated level of capability to conduct terrorist attacks.
- (3) **INTENTIONS:** Recent demonstrated anti-US terrorist activity, or stated or assessed intent to conduct such activity.
- (4) **HISTORY:** Demonstrated terrorist activity over time.
- (5) **TARGETING:** Current credible information on activity indicative of preparations for specific terrorist operations.
- (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 Table V-1.

Table V-1. Threat Level

Critical: Factors 1, 2, and 5 are present.
Factors 3 or 4 may or may not be present.

High: Factors 1, 2, 3, and 4 are present.

Medium: Factors 1, 2, and 4 are present.
Factor 3 may or may not be present.

Low: Factors 1 and 2 are present.
Factor 4 may or may not be present.

Negligible: Factors 1 and/or 2 may or may not be present.

f. Having obtained a threat analysis, the commander and staff proceed to complete the threat and vulnerability assessment. This process considers:

(1) Mission. A review and analysis of the mission of the installation, base, unit, or port in relation to the terrorist threat. The review should assess the cost of antiterrorism measures in terms of lost or reduced mission effectiveness. 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.

(2) Installation, Base, Unit, or Port Assessment. This step combines the results of the following considerations to create the installation, base, unit, or port assessment. The assessment provides the staff with the overall vulnerability to terrorist attack. The staff then develops the crisis management plan (Appendix G) from this assessment. The crisis management plan addresses all terrorist threat levels regardless of the present level. THREATCONS (Appendix J) are then applied in accordance with the local threat. The considerations are:

(a) Vulnerability. The vulnerability assessment (VA) is a self-assessment tool. The installation, base, unit, or port uses the VA to evaluate its vulnerability to terrorist attack. The more vulnerable an installation, base, unit, or port is, the more attractive it becomes to terrorist attack. Appendix B provides a VA format.

(b) Criticality. The criticality assessment identifies key assets and infrastructures located on and adjacent to the installation, base, 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, unit, or port to perform its mission. The staff determines and prioritizes critical assets. The commander approves the prioritized list. The assessment:

1. Selects key assets.
2. Determines whether critical functions

can be duplicated under various attack scenarios.

3. Determines time required to duplicate key assets or infrastructure efforts if temporarily or permanently lost.

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

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

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

(d) 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.

6. Drills and Exercises. Multiechelon wargaming of possible terrorist attacks is the best test, short of an actual incident, to analyze the ability of an installation, base, unit, or port to respond. Drills and exercises test suspected vulnerabilities and antiterrorist 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, unit, or port vulnerabilities.

CHAPTER VI

CRISIS MANAGEMENT EXECUTION

1. General. Chapter IV structured the framework for an integrated antiterrorism 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 include:

- a. Awareness of the possibility of multiple incidents or diversionary tactics.
- b. Activation of required resources by combatant commander and base under attack.
- c. Notifications to the combatant command, appropriate military investigative agency, FBI, and host nation officials.
- d. Exercise of the public affairs officer's role with news media.
- e. Negotiation, if the situation requires it.
- f. Implementation of tactical measures to contain or defeat the threat.
- g. 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.

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 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, 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 operational command, coordination, and control center (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 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 these installation, base, 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 through which an incident may evolve.

a. Phase I is the commitment of locally available resources. This includes available 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 (SRT), emergency services team (EST), FBI regional special weapons and tactics (SWAT) units or the hostage rescue teams (HRTs), 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, 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, DOS and the US Embassy will play the key role in coordinating the US Government and host-country response to such an incident.

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-1.

RESPONSE TO A TERRORIST INCIDENT

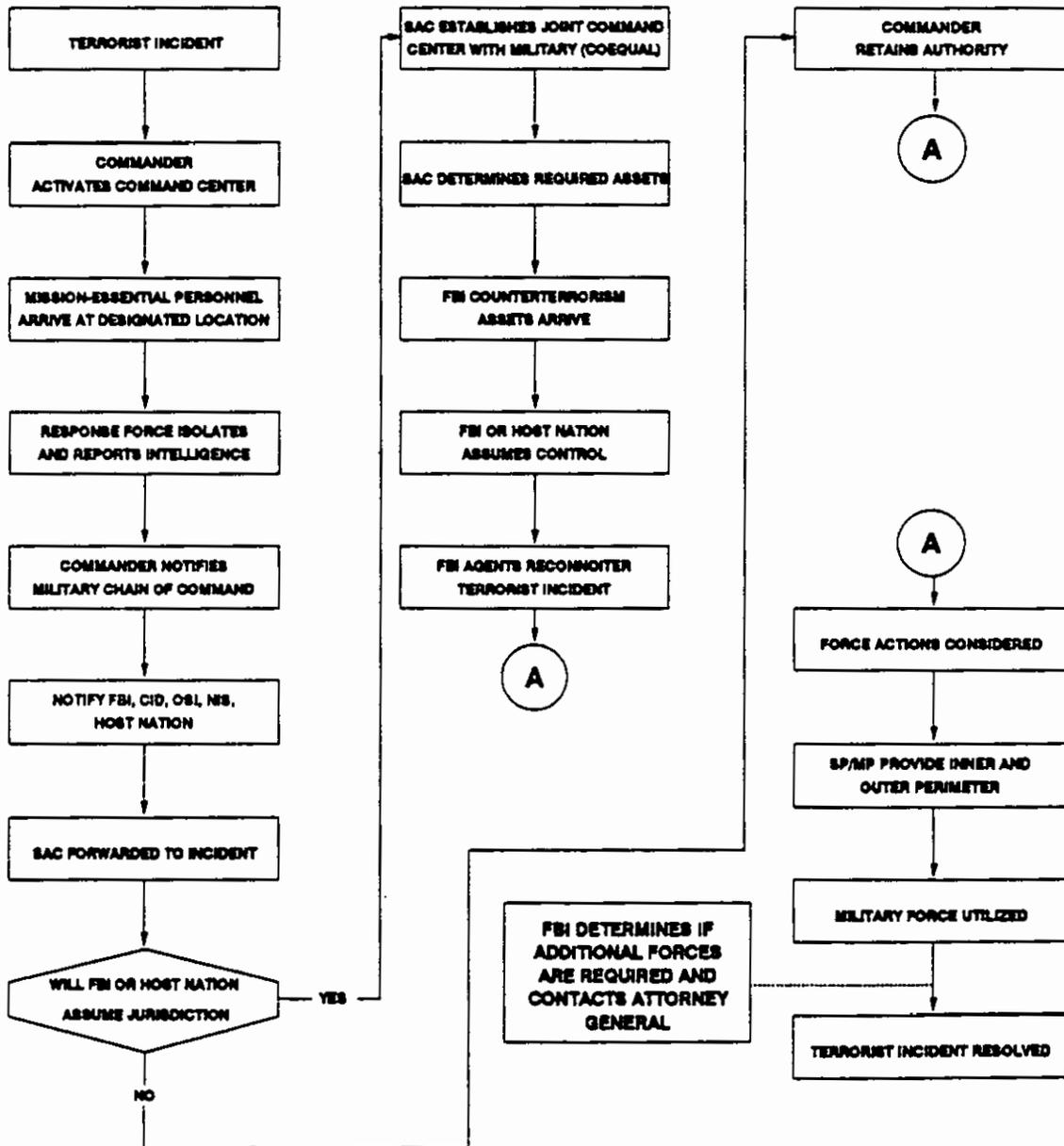


Figure VI-1. Response to a Terrorist Incident

4. Special Considerations. The following special considerations apply in implementing crisis management:

a. Establishing and Controlling Communications. A crucial aspect of implementing the antiterrorist 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 antiterrorism plan. Special SCI communications can be provided by intelligence personnel.

b. Evidence. Witness testimony, photographic evidence, etc., 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 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:

- (1) Photographs and videotapes taken during the incident.
- (2) Physical evidence, including any items used by the terrorists.
- (3) Tape recordings of conversations between terrorists and hostage negotiators.
- (4) Reports prepared by the military law enforcement authorities who initially responded to the incident scene.
- (5) Eyewitness testimony.
- (6) 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, 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 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 this report is in sufficient detail to meet prosecution requirements.

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

- (1) Identify terrorist activities as criminal acts not justifying public support.
- (2) 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.
- (3) Support DOD public affairs strategy on releasing information pertaining to antiterrorism plans, operations, or forces involved in antiterrorist operations.

(a) DOJ has public affairs responsibility for incidents occurring on US territory if the FBI assumes jurisdiction for resolving the incident.

(b) 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, Department of Justice may delegate the public affairs responsibility to a designated DOD representative.

(c) DOS coordinates public affairs during terrorist incidents overseas. DOS may delegate the public affairs responsibility to a designated DOD representative.

(d) 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.

(e) 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 N 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 antiterrorism plan. All personnel involved in the antiterrorism 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 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 with Joint Pub 1-03.30, "Joint After-Action Reporting System."

(INTENTIONALLY BLANK)

CHAPTER VII

PREVENTIVE MEASURES AND CONSIDERATIONS

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. The installation, base, unit, or port antiterrorism 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. Protecting Deployed Forces 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, Sites, and Nonurban 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 the density of buildings, population, or lack of proper cover and concealment. Political restrictions may also limit the military's ability to construct fortifications or disrupt areas. This requires military planners to adapt existing structures to provide protection based on the mission, potential for attack, and ability to use surroundings effectively.

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

(a) 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?

(b) 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) at times can be a valuable source for this information.

(c) Terrain

1. What are the strengths and weaknesses of the installation, base, port, and local surroundings?
2. Are 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?

(d) Troops

1. Determine what is the friendly situation.
2. Are other US forces or equipment available?
3. Are engineers 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?

(e) 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?

(f) 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?

(2) 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. Table VII-1 provides general guidance concerning fortification materials.

Table VII-1. Fortification Materials

<u>Fortification</u>	<u>Materiel</u>	<u>Purpose</u>
Wire fences	Barbed wire	Delay access
	Concertina wire	Channel movement through manned points
	Chain link/weld mesh	Used as grenade, firebomb, or HEAT rocket barriers
Screens	Canvas Plywood	Deny observation
	Natural growth	
Canopies	Chain link/weld mesh	Protect roofs
	Corrugated iron	Detonate mortar projectiles Absorb shrapnel Cover machineguns positioned on roofs
Sandbags	Sandbags	Absorb shrapnel Protect personnel and equipment
Sensors		Provide early warning

(a) Obstacles. Obstacles slow down or disrupt vehicles and personnel approaching an area. Constructing vehicle barriers by using commercially installed electronic barriers, trenches, masonry barriers, concrete-filled oil drums, or vehicles staggered across the route creating a zig-zag 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.

(b) Local Security. Local security must be around-the-clock to provide observation, early warning and, if necessary, live fire capabilities. The security should include guards at entrances to check right of entry in observation posts (OPs), around perimeter, and on rooftops to view the surrounding area. These guard positions must also be integrated into the antiterrorism plan to enable their use in augmenting responding law enforcement personnel. The security force should have available to them, and be trained in the use of, the following equipment in Table VII-2:

Table VII-2. Security Force Equipment

Pyrotechnic pistols	Marshaling 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
Handcuffs	Photographic filter

(4) Specific ROE in the event of civil disturbances, potential damage or injury to US personnel or specific property, looting, or arson.

(5) Response to unauthorized photography.

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

(7) Guidelines for contact with host-nation police.

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

(1) Avoid establishing a regular pattern.

(2) Vary routes and timing.

(3) Travel in groups, never single vehicles.

(4) Avoid traveling at night or during periods of agitation; e.g., religious holidays, political holidays.

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

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

(7) Plan communications requirements.

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

(9) Provide adequate security.

(10) Plan in advance for maintenance and evacuation.

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

(1) Place sandbags on floorboards and fenders.

(2) Cover sandbags with rubber or fiber mats.

- (3) If carrying personnel, sandbag the vehicle bed as well as the driver's compartment.
- (4) Remove canvas so passengers can see and shoot.
- (5) Fold windshield in driver's compartment and fit high-wire cutter.
- (6) Carry no more than one squad per truck.
- (7) Passengers riding in truck bed face outboard and are assigned sectors of observation and fire.
- (8) Rig chicken wire or chain link screens on front bumper frame to deflect rocks, bottles, firebombs, and grenades.
- (9) Carry pioneer tools (fire extinguishers in particular), a line with grappling hook to clear obstacles, and tow bars for disabled vehicles.

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

- (1) Develop and rehearse immediate action drills before movement.
- (2) Perform route clearance before movement.
- (3) Establish and maintain communications throughout the route.
- (4) Develop deception plans to conceal or change movement timing and route; deploy false convoys to contribute to the convoy's security.
- (5) If possible, include host-nation police personnel in the convoy.
- (6) When selecting routes, avoid entering or remaining in dangerous areas. If ambushed, gauge response by enemy strength. Counter ambushes by accelerating through the ambush area, counterattacking, withdrawing, or withdrawing and staging a deliberate attack.
- (7) Convoy escort composition depends on available forces. Light armored vehicles, high mobility multipurpose wheeled vehicles (HMMWV) or trucks equipped with M2 50-caliber and MK19 40mm machineguns 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:

- (a) Determine concept of operation.
- (b) Identify available transportation.
- (c) Identify order of march and road organization.
- (d) Identify disposition of advance guard, main body escort, and reserve.
- (e) Designate assembly area for convoy.
- (f) Determine rendezvous time at assembly area, departure time of first and last vehicle, and expected arrival of first and last vehicle at destination.
- (g) Identify action upon arrival.
- (h) Determine required coordinating instructions for speed, spacing, halts, immediate action drills, breakdowns, and lost vehicles.

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

- (1) Restrict passengers to military personnel only.
- (2) Search for explosives or possible hijackers before departure and after every halt (MWDs are particularly suited for this mission). Appendix N provides information concerning use of MWDs in antiterrorism operations.
- (3) Ensure that the railway is free of obstructions or explosives.
- (4) Patrol the railway area.

- (5) Place armed security personnel on duty throughout the train, including engine room and trail car.
- (6) Patrol and guard departure and arrival stations.
- (7) Use deception measures.
- (8) Provide air cover (AC-130, helicopters).
- (9) Maintain communications within the train and with outside agencies.
- (10) Provide reaction force to be moved by air or coordinate host-nation support (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 threats. Crewmembers must be aware of host-nation support and responsibilities while in port or anchored in foreign national waters. The ship's captain is solely responsible for the ship and all those embarked. As a minimum, the captain:

- (1) Establishes methods of embarkation and debarkation and patrol activities for all personnel.
- (2) Identifies vital areas of the ship (for example, engine room, weapons storage, command and control bridge), and assigns security guards.
- (3) Coordinates above and below waterline responsibilities.
- (4) Establishes a weapons and ammunition policy and ROE, appoints a reaction force; e.g., security alert team (SAT), backup alert force (BAF), reserve force (RF).
- (5) 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:

- (1) Road transport security when driving to and from airfields is critical. Keep arrival arrangements low profile. Do not pre-position road transport at the airport for extended periods before arrival.
- (2) If pre-positioned transport is required, attach a security element and station it within the airfield perimeter. Security at the arrival airfield can be the responsibility of the host nation and requires close coordination. Maintain an open communications net between all elements until the aircraft is loaded and upon arrival, reestablish communications with new security element.
- (3) All personnel (air crews and transported unit) must be cautioned concerning the transportation of souvenirs and other personal items that could be containers for explosives.
- (4) Man-portable weapons systems in the hands of terrorists create additional planning challenges for the security of aircraft. Planning considerations should include defensive measures against such systems in the choosing of airfields, forward arm, and refuel points, etc.

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 emplace 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 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.

k. Observation Posts. OPs provide prolonged observation of areas, people, or buildings. OPs allow observation of an area for possible terrorist activity (avenues of approach); observation of a particular building or street; ability to photograph persons or activities; ability to observe activity before, during, or after a security force operation (e.g., house search) and ability to provide covering fire for patrols. Special factors apply to OPs located in urban areas. The OP party and reaction force must know the procedure, ROE, escape routes, emergency withdrawal procedures, rallying point, casualty evacuation, and password. Cover the occupation and withdrawal of an OP by conducting normal operations (e.g., house searches, roadblocks, patrols to leave people behind), flooding an area with patrols to disguise movement, using civilian vehicles and clothes, 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 excitement and violence; both are highly contagious. Riot control aims to restore order with minimum use of force. 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:

- (1) Flexibility in changing tactics is 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.

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. Appendix K contains procedures for handling bomb situations.

n. Personal Protective Measures. Overseas deployments require a high degree of personal protective measures. The guidelines in Appendix B still apply but the commander must also focus on the exposure of his troops to any special terrorist threat. This requires particular attention to areas where troops will live, work, and conduct rest and recreation. 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 combined 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 antiterrorism measures commensurate with the JRAC's guidance. Specific tactics, techniques, and procedures for operations in the JRA are contained in Joint Pub 3-10.

APPENDIX A

SECTION I. VULNERABILITY ASSESSMENT

1. General. The VA provides the commander with a tool to assess installation, base, unit, or port activity potential vulnerability, but it is not a substitute for sound judgment. The VA must stand on its own and be supported by valid considerations. Typically, a small group of knowledgeable individuals (at a minimum operations, security, intelligence, counterintelligence, communications, and engineer staff personnel) 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 important that the evaluator record assigned points. Installations, bases, units, or ports with a low vulnerability score can still be primary terrorist targets because of one or more of the criteria used. For example, the installation, base, unit, or port may have a very low overall score, but may have scored high on one category (e.g., installation, base, unit, or port characteristics and sensitivity). Terrorists may target the installation, base, unit, or port specifically to obtain nuclear or chemical weapons. Consider each of the VA categories separately. If the installation, base, unit, or port scores high on any of the categories, consider the risk. Even if the score is low on all categories, the risk may still be high if potential terrorist activity exists in the area.

3. Interpretation. No factor is a determinant by itself; the overall relationship between factors must be considered. The VA uses a scale of 0 to 100 points. The higher the value, the higher the vulnerability. Each category has a paragraph for narrative assessment. The narrative paragraph provides a thorough understanding of why and how scores were determined. It is important that the commander fully understand the scoring rationale as well as the reasons certain areas are rated as high risk. The last step involves totaling the points. Review the high scoring areas when determining allotment of resources in order to decrease vulnerability. Upon completion of the VA, total the points in all categories and compare the total to the following scale.

<u>Vulnerability Range</u>	<u>Points</u>
Very low	0 - 10
Low	11 - 30
Medium	31 - 60
High	61 - 80
Very high	81 - 100

**INSTALLATION, BASE, UNIT, OR PORT CHARACTERISTICS
AND SENSITIVITY**
(16 Points Maximum)

Installation, base, unit, or port are capable of establishing and maintaining barrier integrity--especially in emergency situations.

____ VIPs. (1 point per celebrity, 3 points if foreign personnel are present). (6 points maximum)

____ Mission sensitivity. If more than one of the following categories applies, assess maximum point value. (6 points maximum)

Nuclear, chemical, or intelligence facility. (5 points)

Research and development facilities. (4 points)

Designated computer control facilities. (2 points)

Installation, base, post, air station, or air facility. (4 points)

Training facility. (2 points)

____ Current threat analysis by military police, counterintelligence and intelligence personnel. (available = 0 points, unavailable = 3 points)

____ Symbolic value (e.g., museums, historically significant artifacts). (1 point)

NARRATIVE ASSESSMENT:

GEOGRAPHIC REGION
(8 Points Maximum)

Award points based on historical data gathered on terrorist activity by geographic region. Pay special attention to monitoring social unrest and terrorist activity in the local area.

- ___ California, Florida, foreign stations. (8 points)
- ___ Northeast, Mid-Atlantic. (5 points)
- ___ Southwest. (4 points)
- ___ Northwest, Central, Southeast. (2 points)

NARRATIVE ASSESSMENT:

STATUS OF TRAINING
(12 Points Maximum)

Establishing, equipping, maintaining, and testing operations and other special threat personnel are essential. "Trained personnel" refers to response forces, hostage negotiators, crisis management organizations, communications specialists, etc.

- ___ Operations center inactive and no antiterrorism-trained personnel. (12 points)
- ___ Operations center active, but no antiterrorism-trained personnel. (9 points)
- ___ Operations center active, antiterrorism-trained personnel present, but required equipment not available. (7 points)
- ___ Operations center active, antiterrorism-trained personnel present, and required equipment available. (3 points)

_____ Operations center active, antiterrorism-trained personnel present, required equipment available, and system tested semiannually. (0 points)

NARRATIVE ASSESSMENT:

**TIME AND DISTANCE FROM OTHER US MILITARY
INSTALLATIONS/BASES/UNITS/PORTS
(7 Points Maximum)**

Determine points on the ability to obtain assistance in a timely manner.

<u>Time/Distance</u>	<u>Points</u>
No more than 30 minutes/0-20 miles	0
No more than 31-60 minutes/21-45 miles	3
No more than 61-90 minutes/46-70 miles	5
More than 90 minutes/70 miles.....	7

NARRATIVE ASSESSMENT:

**COMMUNICATIONS
(11 Points Maximum)**

Consider security of lines of communication and on-post communications terminals. Consult with the communications officer to accurately assess the vulnerability and operational effectiveness of the communications network.

_____ Communications with lower elements only. (4 points)

- _____ Communications with lower and lateral elements only.
(3 points)
- _____ Communications with higher, lower, and lateral elements.
(0 points)
- _____ Landline telephone.
Nondedicated. (2 points)
Dedicated. (1 point)
Secure dedicated. (0 points)
- _____ Radio.
Nondedicated. (2 points)

Dedicated. (1 point)
Secure dedicated. (0 points)

NARRATIVE ASSESSMENT:

DISTANCE FROM URBAN AREAS
(8 Points Maximum)

For the purposes of this assessment, an urban area has a population of more than 100,000 people. Because of size and the opportunity for the terrorist to blend into the population, urban areas offer the terrorist a safe haven conducive to conducting operations on adjacent military installations, bases, units, or ports.

Distance (miles)	0-10	11-20	21-30	31+
Points	8	6	4	2

NARRATIVE ASSESSMENT:

AVAILABILITY OF NONMILITARY LAW ENFORCEMENT RESOURCES
(8 Points Maximum)

Consider availability of law enforcement agencies, their resources, training status, and response time. Coordinate with agency's point of contact. Plan exercises, and conduct periodic drills to test response time and capabilities.

	<u>Response Time Points</u>			
	<u>1 Hr</u>	<u>2 Hr</u>	<u>3 Hr</u>	<u>+3 Hr</u>
Trained federally* and locally	1	2	3	4
Trained federally*	2	3	4	5
Trained locally	3	4	5	6
Not trained locally	4	5	6	7
Not available	8	8	8	8

* Federally refers to US and host-nation governments.

NARRATIVE ASSESSMENT:

TERRAIN
(6 Points Maximum)

Analyze terrain in conjunction with a review of installation, base, unit, or port sensitivity; adequacy of barrier defense; and routes of ingress or egress.

- ___ Built-up area. (6 points)
- ___ Mountainous, forested, or areas conducive to concealment. (4 points)
- ___ Open areas. (2 points)

NARRATIVE ASSESSMENT:

ACCESS
(8 Points Maximum)

Consider these three methods of entering or exiting both from the terrorist point of view and from that of a unit giving assistance.

- Roads.
 - Freeways. (3 points)
 - Improved roads. (2 points)
 - Secondary roads. (1 point)

- Airfields
 - Usable by high performance (jet) aircraft. (3 points)
 - Usable by low performance (propeller) aircraft. (2 points)
 - Usable by small fixed-wing or rotary-wing aircraft. (1 point)

- Waterways.
 - Navigable. (2 points)
 - Nonnavigable. (1 point)

NARRATIVE ASSESSMENT:

UNITY OF SECURITY EFFORT
(8 Points Maximum)

- Single-Service installation, base, unit, or port and existing crisis management plan and organization.
(0 points)

- Multi-Service installation, base, unit, or port and existing crisis management plan and organization.
(4 points)

_____ Single-Service installation, base, unit, or port and no crisis management plan or organization. (6 points)

_____ Multi-Service installation, base, unit, or port and no existing crisis management plan or organization. (8 points)

NARRATIVE ASSESSMENT:

PROXIMITY TO FOREIGN BORDERS
(8 Points Maximum)

If in the United States, use closest border only. Assess maximum point value, but consider proximity to the borders of nearby foreign countries and their attitude toward terrorists. Thoroughly discuss positive concerns in the narrative assessment.

_____ Mexican border
0-100 miles (8 points)
101-500 miles (6 points)

_____ Canadian border
0-100 miles (6 points)
101-500 miles (4 points)
Over 500 miles (2 points)

NARRATIVE ASSESSMENT:

SECTION II. PORT VULNERABILITY ASSESSMENT

4. General. Ports are highly susceptible to terrorist attacks; therefore, by virtue of their location and mission, the vulnerability assessment requires some additional considerations. This form is a tool to assist field personnel in developing information about individual port areas within their jurisdiction. It is not designed to address every issue or contingency and may be modified, as necessary, for local use.

5. Assessing Vulnerability. To determine port facility vulnerability, 10 major factors are considered:

- a. Port facility characteristics.
- b. Type of security force.
- c. Physical security measures.
- d. Routes of ingress and egress.
- e. Communications.
- f. Availability of additional port security resources.
- g. Response time and distance for security personnel.
- h. Proximity to urban areas.
- i. Geographic location.
- j. Proximity to international borders.

6. Quantification Factors. The "Quantification Factors" follow (point values are not to be interpolated).

Port Passenger Terminal Facility Characteristics and Sensitivity (14 points maximum)

_____ Mission sensitivity. (select best port description)

Dedicated passenger terminal. (3 points)

Military port facility (naval base or military outload terminal (MOT)). (3 points)

Commercial port facility. (2 points)

Petroleum, oils, and lubricants (POL) facility. (1 point)

_____ Current threat analysis.

Unavailable. (3 points)

Available. (0 points)

_____ Port accessibility.

Port facility, uncontrolled access, no gate guard or patrol force. (2 points)

Port facility, controlled access, gate guard, and no patrol force. (1 point)

Port volume capacity. (Measured in tons per year moved if cargo port; passenger ports are measured in passengers per year moved).

CARGO PORT

High (over 25 million tons) (2 points)

Medium (10-25 million tons) (1 point)

Low (under 10 million tons) (0 points)

PASSENGER PORTS

High (over 100,000 passengers) (2 points)

Medium (10,000 to 100,000 passengers) (1 point)

Low (under 10,000 passengers) (0 points)

NOTE: When port is used for both, use highest vulnerability.

_____ DOD Assets Within the Port.

Yes (1 point)

No (0 points)

_____ Civilian Access

Available (3 points)

Unavailable (0 points)

Port Security Force (12 Points Maximum)

Consideration should be given to the type of guard force used (whether contract guard force or state port police), variations in training requirements, and local use of force policy.

- _____ No security guard for trained port facility security personnel. (12 points)
- _____ Port security manager, no security guard force or trained port facility security personnel. (9 points)
- _____ Port security manager, security guard force or port facility security personnel in place but poorly or not trained. (6 points)
- _____ Port security manager, trained port security personnel, not fully equipped. (3 points)
- _____ Port security manager, trained port security personnel, fully equipped. (1 point)
- _____ Port security manager, trained port security personnel, fully equipped, security exercises conducted on a regular schedule. (0 points)

Physical security (12 points maximum)

The following factors should be considered when assigning point values for security systems (landside): barriers, fencing, lighting, vehicle barriers for critical pier areas, and entry control.

- _____ Security systems (landside).
 - No systems. (4 points)
 - Some systems. (2 points)
 - All systems. (0 points)

Consider the following factors when assigning point values for security systems (waterside): patrol craft, surveillance systems, surface search radar, antiswimmer sonar, barriers or nets, and magnetic loop detector or other sensor for submerged delivery vehicles (SDVs).

- _____ Security systems (waterside).
 - No waterside security. (6 points)

- Waterside lighting. (5 points)
- Live surveillance only. (4 points)
- Some technical surveillance. (3 points)
- All combined technical systems only. (2 points)
- All technical systems with live surveillance. (1 point)
- All technical systems with waterside lighting and live surveillance. (0 points)

Analyze terrain within 1 mile in conjunction with a review of ingress or egress route analysis.

_____ Terrain

- Built-up, commercial. (2 points)
- Mountainous, forested, undeveloped. (1 point)
- Open, clear area. (0 points)
- Routes of access and egress. (9 points maximum)

_____ Roads

- Expressways. (3 points)
- Major highways. (2 points)
- Congested city streets. (1 point)

_____ Rail

- Rail gates open at all times. (3 points)
- Rail gates open when in use. (2 points)
- Unused rail access. (1 point)
- No rail access. (0 points)

_____ Water Channels

- More than three chokepoints. (3 points)

1-3 chokepoints. (2 points)

No chokepoints. (1 point)

Communications. (10 points maximum)

Consideration should be given to secure lines of communication. Consultation with the appropriate port authority personnel and local, state, and Federal law enforcement personnel is required to accurately reflect vulnerability and operational effectiveness.

_____ Compatible communications by port authority with:

Local law enforcement agency only. (4 points)

State and local law enforcement agencies. (2 points)

Federal, state, and local law enforcement agencies. (0 points)

_____ Landline telecommunications

Nondedicated. (4 points)

Dedicated point-to-point. (2 points)

Secure dedicated. (0 points)

_____ Radio Communications

Nondedicated. (2 points)

Dedicated. (1 point)

Secure dedicated. (0 points)

Sustainability of Additional Port Security Resources
(8 Points Maximum)

_____ Port security law enforcement resources

<u>Threat</u>	<u>Sustainability (Days)</u>			
	<u>1 Day</u>	<u>3 Days</u>	<u>7 Days</u>	<u>Indefinite</u>
High	8 pts	6 pts	4 pts	2 pts
Medium	7 pts	5 pts	3 pts	1 pt
Low	6 pts	4 pts	2 pts	0 pts

Threat Definitions:

- High: Intelligence indicating an attack of some type will occur within the port.
- Medium: Intelligence indicating an attack of some type may occur within the port.
- Low: Any other intelligence indicating the possibility of terrorist or subversive activity.

**Response Time for Security Personnel Capable of Rendering
Emergency Assistance (7 Points Maximum)**

_____ Response to attack. (4 points)

<u>Response Force</u>	<u>Time To Respond (in minutes)</u>		
	<u>30</u>	<u>30-60</u>	<u>60+</u>
Patrol	2 pts	3 pts	4 pts
Bomb Squad	1 pt	2 pts	3 pts
SWAT	0 pts	1 pt	2 pts

_____ Response to accidents or fire (3 points)

<u>Response Force</u>	<u>Time To Respond (in minutes)</u>		
	<u>15</u>	<u>15-45</u>	<u>45+</u>
Fire Department	1 pt	2 pts	3 pts
Pollution Response Team	0 pts	1 pt	2 pts

Liaison should be maintained with all agencies capable of rendering assistance. Plans should be developed and tested to determine response time and level of capability.

Proximity to Urban Areas (7 Points Maximum)

- _____ Port is surrounded by, and is contiguous to, a heavily populated urban area of over 100,000 people. (7 points)
- _____ Port is surrounded by an area populated by 50,000 to 100,000 people. (6 points)
- _____ Port is surrounded by an area of less than 50,000 people, and the nearest city of greater than 100,000 people is less than 20 miles away. (5 points)
- _____ Port is surrounded by an area of less than 50,000 people, and the nearest city of greater than 100,000 people is 20 to 50 miles away. (4 points)
- _____ Port is surrounded by an area of less than 50,000 people and the nearest city of greater than 100,000 people is more than 100 miles away. (2 points)
- _____ Port is isolated and surrounded by rural undeveloped countryside. (1 point)

Geographic Location (8 Points Maximum)

- _____ Foreign area. (8 points)
- _____ East or west coast. (6 points)
- _____ Gulf coast. (4 points)
- _____ Alaska, northwest, central, and New England. (2 points)

Points are awarded based on historical data gathered on terrorist or subversive activity by geographic region. Special attention should be given to monitoring social unrest and demonstrations in the local areas.

Proximity to International Borders (3 Points Maximum)

For current threat level, refer to Question 1. If no threat assessment is available, assign 3 points.

- _____ High threat area.
0-100 miles (3 points)

101-500 miles (2 points)

+ 500 miles (1 point)

_____ Medium threat area.

0-100 miles (2 points)

101-500 miles (1 point)

+500 miles (0 points)

_____ Low threat area.

0-100 miles (1 point)

101-500 miles (0 points)

+500 miles (0 point)

Islands (0 points)

RANGE OF VULNERABILITY

<u>Very Low</u>	<u>Low</u>	<u>Medium</u>	<u>High</u>	<u>Very High</u>
0-10 pts	11-30 pts	31-55 pts	56-75 pts	76-90 pts

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. 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 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

(1) Encourage security awareness in your family and discuss what to do if there is a security threat.

(2) Be alert for surveillance attempts or suspicious persons or activities, and report them to the proper authorities. Trust your gut feelings.

(3) Vary personal routines whenever possible.

(4) Get into the habit of checking in to let your friends and family know where you are or when to expect you.

(5) Know how to use the local phone system. Always carry telephone change. Know the emergency numbers for local police, fire, ambulance, and hospital.

(6) Know the locations of civilian police, military police, government agencies, US Embassy, and other safe locations where you can find refuge or assistance.

(7) Avoid public disputes or confrontations. Report any trouble to the proper authorities.

(8) 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?"

(9) 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.

(10) 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.

(11) Keep a low profile. Shun publicity. Do not flash large sums of money.

(12) Do not unnecessarily divulge your home address, phone number, or family information.

(13) Watch for unexplained absences of local citizens as an early warning of possible terrorist actions.

(14) 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.

(15) Do not carry sensitive or potentially embarrassing items.

b. At Home

(1) Have a clear view of approaches to your home.

(2) Install strong doors and locks.

(3) Change locks when you move in or when a key is lost.

(4) Install windows that do not allow easy access.

(5) Never leave house or trunk keys with your ignition key while your car is being serviced.

(6) Have adequate lighting outside your house.

(7) Create the appearance that the house is occupied by using timers to control lights and radios while you are away.

(8) Install one-way viewing devices in doors.

Joint Pub 3-07.2

- (9) Install intrusion detection alarms and smoke and fire alarms.
- (10) Do not hide keys or give them to very young children.
- (11) Never leave young children at home alone.
- (12) Never admit strangers to your home without proper identification.
- (13) Use off street parking at your residence, if at all possible.
- (14) Teach children how to call the police, and ensure that they know what to tell the police (name, address, etc.).
- (15) Avoid living in residences that are located in isolated areas, on one-way streets, dead-end streets, or cul-de-sacs.
- (16) Avoid residences that are on the ground floor, adjacent to vacant lots, or on steep hills.
- (17) Carefully screen all potential domestic help.
- (18) Do not place your name on exterior walls of residences.
- (19) Do not answer the telephone with your name and rank.
- (20) Personally destroy all envelopes and other items that reflect personal information.
- (21) Close draperies during periods of darkness. Draperies should be opaque and made of heavy material.
- (22) Avoid frequent exposure on balconies and in windows.
- (23) Consider owning a dog to discourage intruders.
- (24) Never accept unexpected package deliveries.
- (25) Don't let your trash become a source of information.

c. While Traveling

- (1) Vary times and routes.
- (2) Be alert for suspicious-looking vehicles.
- (3) 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).
- (4) Know your driver.
- (5) Equip your car with an inside hood latch and a locking gas cap.
- (6) Drive with windows closed and doors locked.
- (7) Travel with a group of people--there is safety in numbers.
- (8) Travel on busy routes; avoid isolated and dangerous areas.
- (9) Park your car off the street in a secure area.
- (10) Lock your car when it is unattended.
- (11) Do not routinely use the same taxi or bus stop.
NOTE: Buses are preferred over taxis.
- (12) If you think you are being followed, move as quickly as possible to a safe place such as a police or fire station.
- (13) 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.
- (14) Do not pick up hitchhikers.
- (15) Drive on well-lit streets.
- (16) 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.

- (17) Have the driver open the door for you.
- (18) If the driver is absent, do not get into the car.
- (19) If possible, tell your driver your destination only after the car has started.
- (20) Keep your vehicle's gas tank at least half full.

d. In Hotels

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

e. Ground Transportation Security

- (1) Use a plain car that is common in the area to minimize the rich American look.
- (2) Do not be predictable in your daily travel behavior; vary your travel times, your routes, and your mode of transportation whenever possible.
- (3) Check the area around the vehicle, the exterior of the vehicle, and then the interior of the vehicle before starting the engine.
- (4) Travel with companions or in convoy whenever possible.
- (5) Know the locations of safe havens (e.g., police and fire stations) along your travel routes.
- (6) Install appropriate mirrors, locks, and other devices to secure your car against tampering.

- (7) Safeguard car keys at all times.
- (8) 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.
- (9) Lock your car, especially at night, and check and lock your garage when you park there overnight.
- (10) Park in well-lighted areas if you must park on the street.
- (11) Always fasten seat belts, lock doors, and close windows when driving or riding in a car.
- (12) Be alert for surveillance and be aware of possible danger when driving or riding in a car.
- (13) Drive immediately to a "safe haven" when surveillance is suspected; do not drive home.

f. Air Travel Security

- (1) Use military aircraft whenever possible.
- (2) Avoid travel through high-risk areas; use foreign flag airlines and/or indirect routes to avoid such areas.
- (3) Do not use rank or military addresses on tickets, travel documents, hotel reservations, or luggage.
- (4) Select a window seat on aircraft because they offer more protection and are less accessible to hijackers than are aisle seats.
- (5) Select a seat in the midsection of the aircraft because it is not one of the two usual areas of terrorist activity.
- (6) Do not discuss your US Government affiliation with any other passengers.
- (7) 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.

(8) Do not carry classified material unless it is mission-essential.

(9) 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.

(10) Do not carry official papers in your briefcase.

(11) 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.

(12) If possible, check your baggage with the airport's curb service.

(13) 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:

(1) Drop to the floor.

Joint Pub 3-07.2

- (2) Be quiet and do not attract your captors' attention.
- (3) Wait for instructions.
- (4) 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.
- (5) Once released, avoid making comments to the news media until you have been debriefed by the proper US authorities.

(INTENTIONALLY BLANK)

APPENDIX C

VIP AND SENIOR OFFICER SECURITY MEASURES

1. General. VIPs 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 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.

- 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 POV.

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 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.

Joint Pub 3-07.2

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

OFFICE 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 (exterior lights, locks, mirrors, visual devices, etc.) 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 office security programs and frequently conduct security surveys that provide the basis for an effective office 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 office security procedures.

2. Office Accessibility

- a. Offices 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 office 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 high perimeter fence or wall and a comprehensive external lighting system.

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

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

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

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

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

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

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

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

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

- l. Locate outdoor trash containers, storage bins, and bicycle racks away from the building.
 - m. Book depositories or mail slots should not be adjacent to, or in, the building.
 - n. Mailboxes should not be close to the building.
 - o. Seal tops, voids, and open spaces above cabinets, bookcases, and display cases.
 - p. Keep janitorial closets, service openings, telephone closets, and electrical closets locked at all times. Protect communications closets and utility areas with an alarm system.
 - q. Remove names and ranks on reserved parking spaces.
 - r. Empty trash receptacles daily (preferably twice a day).
 - s. Periodically check all fire extinguishers to ensure they are in working order and readily available. Also, periodically check all smoke alarms to ensure they are in working order.
4. Personnel Procedures
- a. Stress heightened awareness by personnel working in the office because effective office 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 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 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 offices 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 office is unattended.

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

n. Lock all office rest rooms when not in use.

o. Escort visitors in the office 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 office 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 (road workers, vendors, etc.), who might station themselves near the office 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 nonorganizational members from bringing boxes and parcels into the building.
- d. Arrange office 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 office'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 performed 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 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.
 - (1) 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.
 - (2) 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.
 - (3) 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 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, 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.

(1) 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.

(2) Other methods of window security include the installation of steel bars, mesh, or grillwork.

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 doorframes 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:

- (1) Strengthen the doorframe by securing 2-inch x 4-inch studs directly behind the doorframe's facing.
- (2) 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 doorframe, it is easily forced apart.
- (3) 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.
- (4) 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

(1) 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.

(2) 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 doorframe.

(3) 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. Usually, rim locks are not 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.

(4) 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 the knob turns freely from the inside to permit rapid exit in case of emergency.

(5) 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

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

(2) Match locks to the door and doorframe to create a strong integral unit.

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

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

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

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

(a) A heavy shackle--at least 9/32-inch of hardened steel.

(b) A double-locking mechanism that locks the heel and toe.

(c) A minimum five-pin tumbler on tumbler locks.

(d) A key-retaining feature that prevents removing the key unless the padlock is locked.

(7) Use rim locks to provide additional protection.

- (8) Lock all vulnerable windows and doors at night.
- (9) Ensure entrance door hinges are heavy duty, pinned in the hinge, and equipped with door pins (metal pins or screws).
- (10) Consider the possible safety hazards of using double-cylinder dead bolt locks that require key action on both sides.
- (11) Check local fire safety codes before using double-cylinder dead bolt locks.
- (12) Fill hollow metal doorframes behind the striker plate with cement to prevent forcing the frame.
- (13) Restrict access or distribution of home and office keys.
- (14) Keep spare keys in a locked drawer or filing cabinet.
- (15) Incorporate heavy-duty, double-cylinder door locks on office entrance doors if fire and safety regulations permit.

(INTENTIONALLY BLANK)

APPENDIX F

TELEPHONE CALL PROCEDURES

1. Upon receiving an anonymous 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 he is indicating his 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 threat information sheet 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 is completed, provide the police duty officer with details of the telephone call and make a full written record of the conversation and your impressions, based on the information annotated on the telephone threat information sheet. This could be invaluable to the local or military police.

TELEPHONE THREAT INFORMATION SHEET

Note: The following information is most commonly needed by police.

Which unit or installation is involved? _____

Nature of the threat. _____

Time or period of the threat. _____

Who made the threat? _____

Date and time of the call. _____

Voice characteristics:

Was the tone normal? _____

Did it sound disguised or muffled? _____

Was it high-pitched or stuttering? _____

Did it sound nervous? _____

Was it slurred or did it indicate that the person was under the influence of alcohol or drugs? _____

Was there evidence of excitement; e.g., hurried speech? _____

Did the caller give the impression that the message was being read? _____

Did the voice have a pronounced or recognizable accent? _____
If so, what type of accent? _____

Apart from establishing the sex of the caller, was there any indication that the person was young or old? _____

Were there background noises? _____ If so:

Was there any sound that would indicate someone else was with the caller; e.g., prompting or giggling in the background? _____

Was there any background noise of road traffic, aircraft, radio, juke box, etc.? _____

Did the caller display a detailed knowledge of the mission or layout of the unit or establishment? _____

Any other pertinent information. _____

Your name: _____

Your organization: _____

Your phone number: _____

(INTENTIONALLY BLANK)

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 OPLANS or CONPLANS prepared by the CINCs to fulfill tasks assigned in the JSCP, or as otherwise directed by the Chairman of the Joint Chiefs of Staff.

CLASSIFICATION

Copy No. _____ of _____ Copies
Issuing Headquarters _____
Location _____
DTG _____

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 operational control 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).

(1) Tactical Situation Possibilities. (Obtained from the commander's planning guidance.)

CLASSIFICATION

CLASSIFICATION

(2) Personnel Situation. (Provided by the personnel officer.)

(3) Logistic Situation. (Provided by the logistics officer.)

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

(5) 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 ensure 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.)

CLASSIFICATION

CLASSIFICATION

b. Material 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.)

(1) Maintenance of Unit Strength

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

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

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

(3) Development and Maintenance of Morale

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

(b) Graves Registration. (Include evacuation procedures and handling of personal effects.)

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

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

CLASSIFICATION

CLASSIFICATION

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 C3 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. Acknowledgment Instructions

/s/
Commander

Annexes as applicable

Distribution:

CLASSIFICATION

(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/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 installation vulnerability determining system when assessing the threat? Does it address:
 - Geography of the area concerned.
 - Law enforcement resources.
 - Population factors.

YES NO

___ ___ Communications capabilities.

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

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?

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 installation's OPSEC program?

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

5. Personnel Security

___ ___ Has an education process been started that identifies threats to vulnerable personnel?

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

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)?

YES NO

- 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?
- 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)?

8. Operations Center Training

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

YES NO

- ___ ___ 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 (e.g., 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?

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-specific 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?

YES NO

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 controlled 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 foreign 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 requirements (e.g., engineer, aviation, medical, communications)?
- Does the plan make provisions for notification of nuclear assessment teams and the nuclear 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?

YES NO

— — Does the plan allow for the purchase and/or use of civilian vehicles, supplies, food; etc., 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?

APPENDIX J

FOR OFFICIAL USE ONLY

THREATCON SYSTEM

SECTION I. BASIC THREATCON PROCEDURES

1. General. The threat conditions (THREATCONS) outlined below describe the progressive level of a terrorist threat to all US military facilities and personnel under DOD Directive O-2000.12. 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 antiterrorism activities. The purpose of the THREATCON system is accessibility to, and easy dissemination of, appropriate information. The declaration, reduction, and cancellation of THREATCONS remain the exclusive responsibility of the commanders specified in the order. 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 antiterrorism plans, recommend that the information contained in this appendix be marked "For Official Use Only" (FOUO) in accordance with DOD Regulation 5400.7-R, October 1990. The DOD Directive O-2000.12 recommended measures are:

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 resulting from intelligence received or as a deterrent. The measures in this THREATCON must be capable of being maintained indefinitely.

(1) 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.

(2) 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.

(3) Measure 3. Secure buildings, rooms, and storage areas not in regular use.

(4) Measure 4. Increase security spot checks of vehicles and persons entering the installation and unclassified areas under the jurisdiction of the United States.

(5) Measure 5. Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.

(6) Measure 6. As a deterrent, apply measures 14, 15, 17, or 18 from THREATCON BRAVO either individually or in combination with each other.

(7) Measure 7. Review all plans, orders, personnel details, and logistic requirements related to the introduction of higher THREATCONs.

(8) Measure 8. Review and implement security measures for high-risk personnel as appropriate.

(9) Measure 9. As appropriate, consult local authorities on the threat and mutual antiterrorism measures.

(10) 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.

(1) Measure 11. Repeat measure 1 and warn personnel of any other potential form of terrorist attack.

- (2) Measure 12. Keep all personnel involved in implementing antiterrorist contingency plans on call.
- (3) Measure 13. Check plans for implementation of the next THREATCON.
- (4) 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.
- (5) Measure 15. Secure and regularly inspect all buildings, rooms, and storage areas not in regular use.
- (6) 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.
- (7) Measure 17. Examine mail (above the regular examination process) for letter or parcel bombs.
- (8) Measure 18. Check all deliveries to messes, clubs, etc. Advise dependents to check home deliveries.
- (9) 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.
- (10) Measure 20. Make staff and dependents aware of the general situation in order to stop rumors and prevent unnecessary alarm.
- (11) Measure 21. At an early stage, inform members of local security committees of actions being taken. Explain reasons for actions.
- (12) 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.
- (13) Measure 23. Operate random patrols to check vehicles, people, and buildings.
- (14) 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.

(15) Measure 25. Implement additional security measures for high-risk personnel as appropriate.

(16) Measure 26. Brief personnel who may augment guard forces on the use of deadly force. Ensure that there is no misunderstanding of these instructions.

(17) Measures 27. As appropriate, consult local authorities on the threat and mutual antiterrorism measures.

(18) Measures 28 and 29. To be determined.

d. THREATCON CHARLIE 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.

(1) Measure 30. Continue, or introduce, all measures listed in THREATCON BRAVO.

(2) Measure 31. Keep all personnel responsible for implementing antiterrorist plans at their places of duty.

(3) Measure 32. Limit access points to the absolute minimum.

(4) Measure 33. Strictly enforce control of entry. Randomly search vehicles.

(5) Measure 34. Enforce centralized parking of vehicles away from sensitive buildings.

(6) Measure 35. Issue weapons to guards. Local orders should include specific orders on issue of ammunition.

(7) Measure 36. Increase patrolling of the installation.

(8) Measure 37. Protect all designated vulnerable points. Give special attention to vulnerable points outside the military establishment.

(9) Measure 38. Erect barriers and obstacles to control traffic flow.

(10) Measure 39. Consult local authorities about closing public (and military) roads and facilities that might make sites more vulnerable to attacks.

(11) 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.

(1) Measure 41. Continue, or introduce, all measures listed for THREATCONs BRAVO and CHARLIE.

(2) Measure 42. Augment guards as necessary.

(3) Measure 43. Identify all vehicles within operational or mission-support areas.

(4) Measure 44. Search all vehicles and their contents before allowing entrance to the installation.

(5) Measure 45. Control access and implement positive identification of all personnel--no exceptions.

(6) Measure 46. Search all suitcases, briefcases, packages; etc., brought into the installation.

(7) Measure 47. Control access to all areas under the jurisdiction of the United States.

(8) Measure 48. Make frequent checks of the exterior of buildings and of parking areas.

(9) Measure 49. Minimize all administrative journeys and visits.

(10) Measure 50. Coordinate the possible closing of public and military roads and facilities with local authorities.

(11) 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.

- (1) Measure 1. Brief crew on the threat, ship security, and security precautions to be taken while ashore.
- (2) Measure 2. Muster and brief security personnel on the threat and rules of engagement.
- (3) Measure 3. Review security plans and keep them available. Keep on call key personnel who may be needed to implement security measures.
- (4) Measure 4. Consistent with local rules, regulations, and status of forces agreement, post qualified armed fantail sentry and forecastle sentry. Rifles are the preferred weapon.
- (5) Measure 5. Consistent with local rules, regulations, and SOFA, post qualified armed pier sentry and pier entrance sentry.

- (6) 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).
- (7) Measure 7. Issue night vision devices to selected posted security personnel.
- (8) 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.
- (9) Measure 9. Tighten shipboard and pier access control procedures. Positively identify all personnel entering pier and fleet landing area--no exceptions.
- (10) Measure 10. Consistent with local rules, regulations, and SOFA, establish unloading zone(s) on the pier away from the ship.
- (11) Measure 11. Deploy barriers to keep vehicles away from the ship. Barriers may be ship's vehicles, equipment, or items available locally.
- (12) Measure 12. Post signs in local language(s) to explain visiting and loitering restrictions.
- (13) Measure 13. Inspect all vehicles entering pier and check for unauthorized personnel, weapons, and/or explosives.
- (14) 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.
- (15) 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.
- (16) 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.

- (17) Measure 17. Identify and inspect workboats.
- (18) Measure 18. Secure spaces not in use.
- (19) Measure 19. Regulate shipboard lighting to best meet the threat environment. Lighting should include illumination of the waterline.
- (20) Measure 20. Rig hawsepipe covers and rat guards on all lines, cable, and hoses. Consider using an anchor collar.
- (21) Measure 21. Raise accommodation ladders, stern gates, jacob ladders, etc., when not in use. Clear ship of all unnecessary stages, camels, barges, oil donuts, and lines.
- (22) Measure 22. Conduct security drills to include bomb threat and repel boarders exercises.
- (23) Measure 23. Review individual actions in THREATCON BRAVO for possible implementation.
- (24) 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.

- (1) Measure 25. Maintain appropriate THREATCON ALPHA measures.
- (2) 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.
- (3) Measure 27. Conduct divisional quarters at foul weather parade to determine the status of on-board personnel and to disseminate information.
- (4) Measure 28. Ensure that an up-to-date list of bilingual personnel for the area of operations is readily available. Ensure 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.

- (5) 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.
- (6) Measure 30. Remind personnel to lock their parked vehicles and to carefully check them before entering.
- (7) 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.
- (8) Measure 32. Consistent with local rules, regulations, and SOFA, establish armed brow watch on pier to check identification and inspect baggage before personnel board ship.
- (9) Measure 33. Man signal bridge or pilot house and ensure flares are available to ward off approaching craft.
- (10) Measure 34. After working hours, place armed sentries on a superstructure level from which they can best cover areas about the ship.
- (11) Measure 35. Arm all members of the quarterdeck watch and SAT. In the absence of a SAT, arm two members of the SDF.
- (12) 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.
- (13) Measure 37. Issue arms to selected qualified officers to include Command Duty Officer (CDO) and Assistant Command Duty Officer (ACDO).
- (14) Measure 38. Arm Sounding and Security Patrol.

(15) Measure 39. Muster and brief ammunition bearers or messengers.

(16) Measure 40. Implement procedures for expedient issue of firearms and ammunition from small arms locker (SAL). Ensure a set of SAL keys are readily available and in the possession of an officer designated for this duty by the commanding officer.

(17) Measure 41. Load additional small arms magazines to ensure adequate supply for security personnel and response forces.

(18) Measure 42. Inform local authorities of actions taken as the THREATCON increases.

(19) Measure 43. Test communications with local authorities and other US Navy ships in port.

(20) Measure 44. Instruct watches to conduct frequent random searches under piers, with emphasis on potential hiding places, pier pilings, and floating debris.

(21) Measure 45. Conduct searches of the ship's hull and boats at intermittent intervals and immediately before it puts to sea.

(22) Measure 46. Move cars and objects such as crates and trash containers 100 feet from the ship.

(23) Measure 47. Hoist boats aboard when not in use.

(24) Measure 48. Terminate all public visits.

(25) Measure 49. Set materiel condition YOKE, main deck and below.

(26) Measure 50. After working hours, reduce entry points to the ship's interior by securing selected entrances from the inside.

(27) Measure 51. Duty department heads ensure all spaces not in regular use are secured and inspected periodically.

(28) Measure 52. If two bows are rigged, remove one of them.

(29) Measure 53. Maintain capability to get under way on short notice or as specified by SOP. Consider

possible relocation sites (different pier, anchorage, etc.). Rig brow and accommodation ladder for immediate raising or removal.

(30) Measure 54. Ensure .50-caliber mount assemblies are in place with ammunition in ready service lockers (.50-caliber machineguns will be maintained in the armory, prefire checks completed, and ready for use).

(31) Measure 55. Prepare fire hoses. Brief designated personnel on procedures for repelling boarders, small boats, and ultralight aircraft.

(32) Measure 56. Obstruct possible helicopter landing areas in such a manner as to prevent hostile helicopters from landing.

(33) Measure 57. Review riot and crowd control procedures, asylum-seeker procedures, and bomb threat procedures.

(34) Measure 58. Monitor local communications (e.g., ship-to-ship, TV, radio, police scanners).

(35) Measure 59. Implement additional security measures for high-risk personnel as appropriate.

(36) Measure 60. Review individual actions in THREATCON CHARLIE for possible implementation.

(37) 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.

(1) Measure 63. Maintain appropriate measures for THREATCONs ALPHA and BRAVO.

(2) Measure 64. Cancel liberty. Execute emergency recall.

(3) Measure 65. Be prepared to get under way on one 1 hour's notice or less. If conditions warrant, request permission to sortie.

- (4) Measure 66. Muster and arm SAT, BAF, and reserve force (RF). Position SAT and BAF at designated location(s). Deploy RF to protect command structure and augment posted security watches.
- (5) Measure 67. Place armed sentries on a superstructure level from which they can best cover areas about the ship.
- (6) Measure 68. Establish .50- or .30-caliber machine-gun positions.
- (7) Measure 69. If available, deploy STINGER surface-to-air missiles IAW established ROE.
- (8) Measure 70. Energize radar and establish watch.
- (9) 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.
- (10) Measure 72. Man one or more repair lockers. Establish communications with an extra watch in DC Central.
- (11) Measure 73. Deploy picket boat. Boats should be identifiable night and day from the ship (e.g., by lights or flags).
- (12) Measure 74. If feasible, deploy a helicopter as an observation or gun platform. The helicopter should be identifiable night and day from the ship.
- (13) Measure 75. Activate antiswimmer watch. (Portions of watch may already be implemented by previous THREATCON measures).
- (14) Measure 76. Issue weapons to selected officers and chief petty officers in the duty section (i.e., the commanding officer, executive officer, department heads).
- (15) Measure 77. Issue concussion grenades to topside rovers, forecastle and fantail sentries, and bridge watch.

- (16) Measure 78. Erect barriers and obstacles as required to control traffic flow.
- (17) Measure 79. Strictly enforce entry control procedures and searches--no exceptions.
- (18) Measure 80. Enforce boat exclusion zone.
- (19) Measure 81. Minimize all off-ship administrative trips.
- (20) Measure 82. Discontinue contract work.
- (21) Measure 83. Set materiel condition ZEBRA, second deck and below.
- (22) Measure 84. Secure from the inside all unguarded entry points to the interior of the ship.
- (23) Measure 85. Rotate screws and cycle rudder(s) at frequent and irregular intervals.
- (24) Measure 86. Rig additional firehoses. Charge the firehoses when manned just prior to actual use.
- (25) Measure 87. Review individual actions in THREATCON DELTA for implementation.
- (26) 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.

- (1) Measure 89. Maintain appropriate THREATCONs ALPHA, BRAVO, and CHARLIE measures.
- (2) Measure 90. Permit only necessary personnel topside.
- (3) Measure 91. Prepare to get under way and, if possible, cancel port visit and depart.
- (4) Measure 92. Post sentries with M60 machinegun(s) to cover possible helicopter landing areas.
- (5) Measure 93. Arm selected personnel of the SDF.

(6) Measure 94. Deploy M-79 grenade launchers to cover approaches to ship.

(7) 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

(1) Planning

(a) Review THREATCONS ALPHA and BRAVO measures.

(b) Update THREATCONS ALPHA and BRAVO measures as required.

(2) Briefing and Liaison

(a) Brief all personnel on the threat, especially pilots, ground support crews, and air traffic controllers.

(b) Inform local police of the threat. Coordinate plans to safeguard aircraft flight paths into and out of air stations.

(c) Ensure duty officers are always available by telephone.

(d) Prepare to activate contingency plans and issue detailed air traffic control procedures if appropriate.

(e) Be prepared to receive and direct aircraft from other stations.

(3) Precautions Inside the Perimeter

(a) Perform thorough and regular inspection of areas within the perimeters from which attacks on aircraft can be made.

Joint Pub 3-07.2

(b) Take action to ensure no extremists armed with surface-to-air missiles can operate against aircraft within the perimeter.

(c) Establish checkpoints at all entrances and inspect all passes and permits. Identify documents of individuals entering the area--no exceptions.

(d) Search all vehicles, briefcases, packages, etc., entering the area.

(e) Erect barriers around potential targets if at all possible.

(f) Maintain firefighting equipment and conduct practice drills.

(g) Hold practice alerts within the perimeter.

(4) Precautions Outside the Perimeter

(a) Conduct, with local police, regular inspections of the perimeter--especially the area adjacent to flight paths.

(b) 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.

(c) Advise aircrews to report any unusual activity near approach and overshoot areas.

b. THREATCON CHARLIE

(1) Planning

(a) Review THREATCON CHARLIE measures.

(b) Update THREATCON CHARLIE measures as required.

(2) Briefing and Liaison

(a) Brief all personnel on the increased threat.

(b) Inform local police of increased threat.

(c) Coordinate with the local police on any precautionary measures taken outside the airfield's perimeters.

(d) Implement appropriate flying countermeasures specified in SOPs when directed by air traffic controllers.

(3) Precautions Inside the Perimeter

(a) Inspect all vehicles and buildings on a regular basis.

(b) Detail additional guards to be on call at short notice and consider augmenting firefighting details.

(c) Carry out random patrols within the airfield perimeter and maintain continuous observation of approach and overshoot areas.

(d) Reduce flying to essential operational flights only. Cease circuit flying if appropriate.

(e) Escort all visitors.

(f) Close relief landing grounds where appropriate.

(g) Check airfield diversion state.

(4) Precautions Outside the Perimeter

(a) Be prepared to react to requests for assistance.

(b) Provide troops to assist local police in searching for terrorists on approaches outside the perimeter of military airfields.

c. THREATCON DELTA

(1) Planning

(a) Review THREATCON DELTA measures.

(b) Update THREATCON DELTA measures as required.

(2) Briefings and Liaison

(a) Brief all personnel on the very high levels of threat.

- (b) Inform local police of the increased threat.
- (3) Precautions Inside the Perimeter
- (a) Cease all flying except for specifically authorized operational sorties.
 - (b) Implement, if necessary, appropriate flying countermeasures.
 - (c) Be prepared to accept aircraft diverted from other stations.
 - (d) Be prepared to deploy light aircraft and helicopters for surveillance tasks or to move internal security forces.
- (4) Precautions Outside the Perimeter. Close military roads allowing access to the airbase.

(INTENTIONALLY BLANK)

APPENDIX K

EXPLOSIVE DEVICE PROCEDURES

1. Appropriate responses to take when a suspected IED is discovered are outlined below.

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 G 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.

(1) Factors favoring a search before movement of personnel include the following:

(a) High incidence of hoax telephone threats.

(b) Effective security arrangements have been established.

(c) Information in the warning is imprecise or incorrect.

(d) Caller sounded intoxicated, amused, or very young.

(e) Prevailing threat of terrorist activity is low.

(2) Factors favoring movement of personnel before searching include the following:

(a) The area (e.g., post or base) is comparatively open.

(b) Information in the warning is precise as to matters of location, description of device, timing, and motive for attack.

(c) Prevailing threat of terrorist activity is high.

c. Searching for a Suspected IED

(1) Use a **nominated persons search** when the threat's credibility is very low. The search is possible in a short time or can be done covertly. Predesignated individuals search assigned areas.

(2) 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.

(3) Use a **team search** when the threat's credibility is high. The search is very thorough and places the minimum number of personnel at risk. Completely evacuate the area and ensure it remains evacuated until the search is complete. Search teams make a systematic search of the area. The search is slow and thorough.

(4) Use **MWD bomb dog team**, if available, as a final means of checking the situation in each instance.

d. Search Procedures

(1) Make an audio check and listen for unusual sounds.

(2) Visually sweep the area up to the waist, then sweep up to the ceiling. Do not forget the tops of cabinets and cupboards.

(3) Perform a thorough and systematic search in and around containers and fixtures.

(4) 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, marshaling, 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:

(1) Assembly areas should be at least 200 meters, and not less than 100 meters, from the likely target or building, if at all possible.

(2) Locate assembly areas in areas where there is little chance of an IED being hidden. Open spaces are best. Avoid car parking areas because IEDs can be easily hidden in vehicles.

(3) 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.

(4) 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 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 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.

1. 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. ICP and Cordon. Cordon suspicious objects to a distance of at least 100 meters and cordon suspicious vehicles to a distance of at least 200 meters. Ensure 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 reoccupation of an evacuated facility rests with the cognizant commander or senior DOD civilian in charge of the facility.

3. 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.

4. Reaction to an Exploded IED

a. Explosion Without Casualties

- (1) Maintain the cordon. Allow only authorized personnel into the explosion area.
- (2) Fight any fires threatening undamaged buildings if this can be achieved without risking personnel.
- (3) Report the explosion to the military law enforcement authorities or local police if they are not yet in attendance.
- (4) 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.
- (5) Ensure a clear passage for emergency vehicles (e.g., fire trucks, ambulances) and corresponding personnel is maintained.
- (6) Refer media inquiries to the PAO at the operations center.
- (7) 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 to 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

- (1) 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.

- (2) Include the following information in your report:
- (a) Any warning received and if so, how it was received.
 - (b) Identity of the person(s) who discovered the device.
 - (c) How the device was discovered; e.g., casual discovery, organized search.
 - (d) Location of the device--give as much detail as possible.
 - (e) Time of discovery.
 - (f) Estimated length of time the device has been in its location.
 - (g) Description of the device--give as much detail as possible.
 - (h) Safety measures taken.
 - (i) Suggested routes to the scene.
 - (j) Any other pertinent information.
- (3) Access control.
- (a) Upon arrival, ensure military law enforcement authorities, local police, and EOD vehicles are not impeded from reaching the ICP.
 - (b) Evacuate through building doors and windows.
 - (c) 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.
 - (d) 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

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	FBI/NIS/PMO
OFF BASE	CIVIL POLICE	FBI/ CIVIL POLICE	FBI/ CIVIL POLICE	(SUPPORT FBI)	CID AFOBI FBI
OUTSIDE THE UNITED STATES					
ON BASE	MILITARY POLICE	HOST GOVERNMENT/DOS INSTALLATION COMMANDER	HOST GOVERNMENT/DOS INSTALLATION COMMANDER	INSTALLATION OR UNIT COMMANDER (LAW APPLICABLE STATUS OF FORCES AGREEMENT OR OTHER BILATERAL AGREEMENTS GOVERNING THE EMPLOYMENT OF MILITARY FORCES)	HOST GOVERNMENT/NIS/PMO CID OSI
OFF BASE	HOST-COUNTRY LAW ENFORCEMENT	HOST GOVERNMENT/ DOS	HOST GOVERNMENT/ DOS	INSTALLATION OR UNIT COMMANDER (LAW 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 support procedures are in place and established information/communication channels are functioning.

(INTENTIONALLY BLANK)

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 commander, other operations center staff, and higher echelon PAOs before release.
- ___ Control movement of news media personnel with press passes, escorts, etc.
- ___ 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 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 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 antiterrorism requirements. The military law enforcement office supporting your area should be consulted for specifics associated with using MWDs in your area of responsibility.

2. General. The DOD MWD program produces three types of trained MWDs: patrol-narcotics, patrol-explosives, and patrol. All three types are excellent for use in an antiterrorism 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. It will increase the speed of many operations and by its ability to locate at a distance in the right conditions, it can enhance the effectiveness of searches and patrols. The MWD is an excellent deterrent in many circumstances.

4. Disadvantages. An MWD can be detracted 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 antiterrorism 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 antiterrorism plans. The following are some of the possibilities:

- a. Patrolling perimeters and critical facilities.
- b. Searching for explosives.
- c. Augmenting access control points.

- d. Deterrent in riot and crowd control situations.
- e. Early warning indicator for intrusions.
- f. Augmentation to military law enforcement capabilities.

6. Legal Considerations. The military law enforcement office will coordinate with appropriate command legal authorities to determine ROE for MWD in a particular area. These ROE should be spelled out in the antiterrorism plan and practiced during training exercises.

APPENDIX O

USER'S EVALUATION REPORT
ON JOINT PUB 3-07.2

1. Users in the field are highly encouraged to submit comments on this pub. Please fill out the following: User's POC, unit address, and phone (DSN) number.

2. Content

a. Does the pub provide a conceptual framework for the topic? _____

b. Is the information provided accurate? What needs to be updated? _____

c. Is the information provided useful? If not, how can it be improved? _____

d. Is this pub consistent with other joint pubs? _____

e. Can this pub be better organized for the best understanding of the doctrine and/or JTTP? How? _____

3. Writing and Appearance

a. Where does the pub need some revision to make the writing clear and concise? What words would you use? _____

b. Are the charts and figures clear and understandable? How would you revise them? _____

4. Recommended urgent change(s) (if any). _____

5. Other _____

6. Please fold and mail comments to the Joint Doctrine Center (additional pages may be attached if desired) or FAX to DSN 564-3990 or COMM (804) 444-3990.

(FOLD)

JOINT DOCTRINE CENTER
BLDG R-52
1283 CV TOWWAY STE 100
NORFOLK, VA 23511-2491

(FOLD)

APPENDIX O

**USER'S EVALUATION REPORT
ON JOINT PUB 3-07.2**

1. Users in the field are highly encouraged to submit comments on this pub. Please fill out the following: User's POC, unit address, and phone (DSN) number.

2. Content

a. Does the pub provide a conceptual framework for the topic? _____

b. Is the information provided accurate? What needs to be updated? _____

c. Is the information provided useful? If not, how can it be improved? _____

d. Is this pub consistent with other joint pubs? _____

e. Can this pub be better organized for the best understanding of the doctrine and/or JTTP? How? _____

3. Writing and Appearance

a. Where does the pub need some revision to make the writing clear and concise? What words would you use? _____

b. Are the charts and figures clear and understandable? How would you revise them? _____

4. Recommended urgent change(s) (if any). _____

5. Other _____

6. Please fold and mail comments to the Joint Doctrine Center (additional pages may be attached if desired) or FAX to DSN 564-3990 or COMM (804) 444-3990.

(FOLD)

JOINT DOCTRINE CENTER
BLDG R-52
1283 CV TOWWAY STE 100
NORFOLK, VA 23511-2491

(FOLD)

APPENDIX O

**USER'S EVALUATION REPORT
ON JOINT PUB 3-07.2**

1. Users in the field are highly encouraged to submit comments on this pub. Please fill out the following: User's POC, unit address, and phone (DSN) number.

2. Content

a. Does the pub provide a conceptual framework for the topic? _____

b. Is the information provided accurate? What needs to be updated? _____

c. Is the information provided useful? If not, how can it be improved? _____

d. Is this pub consistent with other joint pubs? _____

e. Can this pub be better organized for the best understanding of the doctrine and/or JTTP? How? _____

3. Writing and Appearance

a. Where does the pub need some revision to make the writing clear and concise? What words would you use? _____

b. Are the charts and figures clear and understandable? How would you revise them? _____

4. Recommended urgent change(s) (if any). _____

5. Other _____

6. Please fold and mail comments to the Joint Doctrine Center (additional pages may be attached if desired) or FAX to DSN 564-3990 or COMM (804) 444-3990.

(FOLD)

JOINT DOCTRINE CENTER
BLDG R-52
1283 CV TOWWAY STE 100
NORFOLK, VA 23511-2491

(FOLD)

APPENDIX O

**USER'S EVALUATION REPORT
ON JOINT PUB 3-07.2**

1. Users in the field are highly encouraged to submit comments on this pub. Please fill out the following: User's POC, unit address, and phone (DSN) number.

2. Content

a. Does the pub provide a conceptual framework for the topic? _____

b. Is the information provided accurate? What needs to be updated? _____

c. Is the information provided useful? If not, how can it be improved? _____

d. Is this pub consistent with other joint pubs? _____

e. Can this pub be better organized for the best understanding of the doctrine and/or JTTP? How? _____

3. Writing and Appearance

a. Where does the pub need some revision to make the writing clear and concise? What words would you use? _____

b. Are the charts and figures clear and understandable? How would you revise them? _____

4. Recommended urgent change(s) (if any). _____

5. Other _____

6. Please fold and mail comments to the Joint Doctrine Center (additional pages may be attached if desired) or FAX to DSN 564-3990 or COMM (804) 444-3990.

(FOLD)

JOINT DOCTRINE CENTER
BLDG R-52
1283 CV TOWWAY STE 100
NORFOLK, VA 23511-2491

(FOLD)

APPENDIX O

**USER'S EVALUATION REPORT
ON JOINT PUB 3-07.2**

1. Users in the field are highly encouraged to submit comments on this pub. Please fill out the following: User's POC, unit address, and phone (DSN) number.

2. Content

a. Does the pub provide a conceptual framework for the topic? _____

b. Is the information provided accurate? What needs to be updated? _____

c. Is the information provided useful? If not, how can it be improved? _____

d. Is this pub consistent with other joint pubs? _____

e. Can this pub be better organized for the best understanding of the doctrine and/or JTTP? How? _____

3. Writing and Appearance

a. Where does the pub need some revision to make the writing clear and concise? What words would you use? _____

b. Are the charts and figures clear and understandable? How would you revise them? _____

4. Recommended urgent change(s) (if any). _____

5. Other _____

6. Please fold and mail comments to the Joint Doctrine Center (additional pages may be attached if desired) or FAX to DSN 564-3990 or COMM (804) 444-3990.

(FOLD)

JOINT DOCTRINE CENTER
BLDG R-52
1283 CV TOWWAY STE 100
NORFOLK, VA 23511-2491

(FOLD)

GLOSSARY

PART I--ABBREVIATIONS AND ACRONYMS

ACDO	Assistant Command Duty Officer
AFOSI	Air Force Office of Special Investigations
AIQC	Antiterrorism Instructor Qualification Course
ASD (SO/LIC)	Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict)
BAF	backup alert force
C3I	command, control, communications, and intelligence
CCB	Community Counterterrorism Board
CDO	Command Duty Officer
CIA	Central Intelligence Agency
CID	Criminal Investigation Division
CINC	commander of a unified or specified command
CISO	Counterintelligence Support Officer
COMSEC	communications security
CONUS	continental United States
CT	counterterrorism
DIA	Defense Intelligence Agency
DOE	Department of Energy
DOJ	Department of Justice
DON	Department of the Navy
DOS	Department of State
DOT	Department of Transportation
EOD	explosive ordnance disposal
EEFI	essential elements of friendly information
EI	essential elements of information
EST	emergency service team
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FOUO	For Official Use Only
HEAT	high explosive antitank
HMMWV	high mobility multipurpose wheeled vehicle
HQMC	Headquarters, US Marine Corps
HQMC(CIC)	Headquarters, US Marine Corps, Counterintelligence
HQMC(CID)	Headquarters, US Marine Corps, Criminal Investigations Division
HRT	hostage rescue team
IAW	in accordance with
ICP	incident control point

IED improvised explosive device
 INSCOM US Army Intelligence and Security Command
 INTAC Individual Terrorism Awareness Course
 IOC Investigations Operations Center

 JRA joint rear area
 JRAC joint rear area coordinator
 JS Joint Staff
 JTF joint task force
 JTTP joint tactics, techniques, and procedures

 LIC low-intensity conflict

 MOU memorandum of understanding
 MWD military working dog

 NAVATAC Navy Antiterrorism Analysis Center
 NISCOM Naval Investigative Service Command
 NMCC National Military Command Center
 NMCS National Military Command System
 NSA National Security Agency
 NSC National Security Council
 NSD National Security Directive
 NSDD National Security Decision Directive

 OCONUS outside continental United States
 OP observation post
 OPSEC operations security

 PAO public affairs office
 PMO provost marshal office
 POL petroleum, oils, and lubricants
 POV privately owned vehicle

 RF Reserve force
 ROE rules of engagement

 SAC Special Agent in Charge
 SAL small arms locker
 SAT security alert team
 SCI sensitive compartmented information
 SDF self defense force
 SDV submerged delivery vehicle
 SOP standing/standard operating procedure
 SOFA status-of-forces agreement
 SRT special reaction team
 SWAT special weapons and tactics

 THREATCON threat condition
 USACIDC US Army Criminal Investigations Command

USAITAC US Army Intelligence Threat Analysis Center
USAJFKSWCS US Army John F. Kennedy Special Warfare
Center
USAMPS US Army Military Police School
USAF US Air Force
USCG US Coast Guard
USMC US Marine Corps

VIP very important person
VA vulnerability assessment

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. (Approved for inclusion in the next edition of 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. (Approved for inclusion in the next edition of 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 for or on behalf of foreign powers, organizations, or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs. (Approved for inclusion in the next edition of 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)

high-risk personnel. Personnel who, because of their grade, assignment, symbolic value, or relative isolation, are likely to be attractive or accessible terrorist targets. (Approved for inclusion in the next edition of 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)

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. (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. (Approved for inclusion in the next edition of 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. (Approved for inclusion in the next edition of Joint Pub 1-02)

insurgency. An organized movement aimed at the overthrow of a constituted government through use of subversion and armed conflict. (Joint Pub 1-02)

insurgent. Member of a political party who rebels against established leadership. (Approved for inclusion in the next edition of Joint Pub 1-02)

National Command Authorities. The President and the Secretary of Defense or their duly deputized alternates or successors. Commonly referred to as NCA. (Joint Pub 1-02)

negotiations. A discussion between authorities and a barricaded offender or terrorist to effect hostage release and terrorist surrender. (Approved for inclusion in the next edition of Joint Pub 1-02)

open source information. Information of potential intelligence value (i.e., intelligence information) that is available to the general public. (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. (Approved for inclusion in the next edition of Joint Pub 1-02)

operations security. A process of identifying critical information and subsequently analyzing friendly actions attendant to 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. (Approved for inclusion in the next edition of 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. (Approved for inclusion in the next edition of Joint Pub 1-02)

primary target. An object of high publicity value to terrorists. (Approved for inclusion in the next edition of Joint Pub 1-02)

proactive. Measures taken in the preventive stage of antiterrorism designed to harden targets and detect actions before they occur. (Approved for inclusion in the next edition of Joint Pub 1-02)

revolutionary. An individual attempting to effect a social or political change through the use of extreme measures. (Approved for inclusion in the next edition of Joint Pub 1-02)

saboteur. One who commits sabotage. (Approved for inclusion in the next edition of Joint Pub 1-02)

secondary targets. Alternative targets of lower publicity value. Attacked when primary target is unattainable. (Approved for inclusion in the next edition of Joint Pub 1-02)

signal security. A generic term that includes both communications security and electronic security. (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. (Approved for inclusion in the next edition of Joint Pub 1-02)

tactical security. In operations, the measures necessary to deny information to the enemy and to ensure that a force retains its freedom of action and is warned or protected against an unexpected encounter with the enemy or an attack. (Approved for inclusion in the next edition of Joint Pub 1-02)

terrorism. The calculated use or 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. (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. (Approved for inclusion in the next edition of 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. (Approved for inclusion in the next edition of 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 that 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. (Approved for inclusion in the next edition of Joint Pub 1-02)

threat and vulnerability assessment. In antiterrorism, the pairing of a facility's threat analysis and vulnerability

analysis. (Approved for inclusion in the next edition of Joint Pub 1-02)

terrorist threat conditions. A CJCS-approved program standardizing the Military Services' identification of and recommended responses to terrorist threats against US personnel and facilities. Also called THREATCONs, this program facilitates inter-Service coordination and support for antiterrorism activities. 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. (Approved for inclusion in the next edition of Joint Pub 1-02)